UNIVERSIDAD CARLOS III DE MADRID

TRABAJO FIN DE GRADO

ANÁLISIS DE LAS VULNERABILIDADES DE LOS SISTEMAS AUTOMÁTICOS DE FRONTERAS (SISTEMAS ABC)

GRADO EN INGENIERÍA ELECTRÓNICA INDUSTRIAL Y AUTOMÁTICA

Autor: Jorge Gutierrez Ruiz

Tutor: Raúl Sánchez Reíllo

Leganés, 20 de Junio de 2014

“Todos hacemos decisiones, pero al final, las decisiones nos hacen a nosotros”

- Andrew Ryan

Agradecimientos

En primer lugar, me gustaría dar las gracias a Belén Fernández por guiarme siempre en la realización de este proyecto, por su tiempo y el esfuerzo que me ha dedicado. A Raúl Sánchez Reíllo, mi tutor y a todo el Grupo Universitario de Tecnologías de Identificación de la universidad por brindarme esta oportunidad y por ayudarme en todo lo posible siempre que lo he necesitado. Agradezco también a todos los profesores que he tenido, desde el colegio hasta la universidad, por lo que para bien o para mal, cada uno ha aportado algo en mi educación, consiguiendo que hoy sea quién soy y esté donde estoy. En especial a mis profesores Vicente, Carmen y Montoro, que cambiaron mi forma de ver las cosas y por supuesto, a la "élite" del GsD.

Quiero agradecerle este trabajo a la gente sin la cual sería imposible estar escribiéndolo hoy pues la entrega de este proyecto simboliza el fin de cuatro años compartiendo momentos inolvidables. Han sido inolvidables porque cada uno de vosotros ha aportado algo que ha hecho especial el camino. Gracias al cheto: el Turas, Varo, Babi, Montejo, el Potas, Ctor, Ojeda, Jesus, Juan, Perraco y Sebix. Gracias a mis compañeros de clase: Stan, Lestón, Oscar, Jesús, Jaime y Left. Gracias a mis grandes amigas y consejeras Adriana e Isabel. Gracias a todos por hacerme estos últimos años mucho más llevaderos.

Martina, gracias. No voy a olvidar tu apoyo y tus consejos. Gracias por todo lo que me has ayudado, sabes que siempre me sentiré en deuda contigo.

Y sobretodo gracias a mi gran familia: Mi madre Carmen, mi padre Fernando, Santi, Ángeles y a mis dos hermanas, Ana y María. Gracias por enseñarme todo lo que sabéis, ayudarme en todo lo que habéis podido, darme todo lo que habéis tenido y quererme tanto. Este proyecto también es el fruto de vuestro esfuerzo.

Por último, te dedico este proyecto a tí, abuela, por ser mi modelo de tesón y coraje. Me hiciste ser mejor persona.

Gracias a todos.

Resumen

Desde los años 60 se han desarrollado cada vez más, sistemas automáticos de identificación basados en técnicas biométricas. Estas técnicas de reconocimiento tienen un gran interés porque suponen una forma segura y sencilla de identificar a personas; lo que hacía posible abandonar los sistemas tradicionales que conllevaban riesgos de seguridad importantes (tarjetas de identificación y/o contraseñas que pueden ser perdidas, olvidadas o sustraídas). Por ello, los sistemas biométricos han experimentado un enorme crecimiento y actualmente están presentes en multitud de escenarios: control de pasajeros en aeropuertos, autenticación de documentos, Smartphone, control de acceso a zonas restringidas, control de asistencia laboral, etc.

Sin embargo, a pesar del aumento del uso de sistemas biométricos no es una práctica común su evaluación para que cumplan ciertos requisitos de rendimiento y/o de seguridad. Esto se debe a que evaluar un sistema biométrico es un reto muy difícil porque cualquier característica del sistema requiere controlar muchos factores, lo cual conlleva un proceso muy complejo.

En este Trabajo de Fin de Grado (TFG) se van a utilizar las metodologías de evaluación existentes para unificarlas, desarrollarlas y complementarlas para así definir una metodología general completa para la evaluación de la seguridad de un sistema biométrico.

También serán objeto de estudio los sistemas automáticos de control de fronteras (sistemas ABC). Dichos sistemas controlan los accesos y cruces fronterizos de forma automatizada en una gran cantidad de aeropuertos del mundo. Puesto que dichos sistemas son muy importantes debido a su aplicación, se analizarán las vulnerabilidades de los sistemas ABC aplicando la metodología para la evaluación de la seguridad desarrollada y añadiendo nuevos aspectos característicos del control de fronteras.

El presente documento introduce al lector a los sistemas biométricos y describe el proceso de desarrollo de la metodología completa para la evaluación de la seguridad aplicándolo en última instancia, a los sistemas automáticos de control de fronteras o sistemas ABC.

Abstract

Since the 60´s, the automatic identification based on biometric techniques increased tremendously. This kind of techniques had a big interest because of its safety and easily way to identify people and because it makes possible to forget about the traditional systems full of vulnerabilities (ID cards or passwords that can be robbed, forgotten or lost). Because of this, the biometric systems are now present in lots of applications: border control at the airports, Smartphone, access control, etc.

However, in spite of the highly increasing usage in these kinds of systems, it's not a common practice evaluate its performance and/or security. This is because the task of evaluate a biometric system is a challenging issue because any characteristic of the system requires controlling of many factors, which makes the task harder.

In this Bachelor thesis are going to be used the existing methodologies for evaluation but also they are going to be unified, developed and completed so a new complete and general methodology will be defined for the security evaluation of biometric systems.

The automated border control systems (ABC systems) will be studied as well. These systems take care of the border crossing in most of the airports all over the world. Because of its importance and its application field, the new developed methodology will be applied to the ABC systems and also complemented with particular aspects about the border control processing.

This document introduces the reader to the biometric systems and describes the entire process of development in the complete methodology for security evaluation, applying it at the end, to the ABC systems.

Índice

Índice de Figuras

Índice de Tablas

Listado de Acrónimos

GUTI	Grupo Universitario de Tecnologías de Identificación
TFG	Trabajo Fin de Grado
UC3M	Universidad Carlos III de Madrid
BEM	Biometric Evaluation Methodology / Metodología de evaluación biométrica
ABC	Automated Border Control / Control Automático de Fronteras
ROC	Receiver Operating Characteristic / Característica Operativa del Receptor
FAR	False Accept Rate / Tasa de Falsa Aceptación
FRR	False Reject Rate / Tasa de Falso Rechazo
EER	Equal Error Rate / Tasa de Error de Cruce
RF	Radio frecuencia
FTA	Failure to Acquire / Fallo a Adquirir
FTC	Failure to Capture / Fallo a Capturar
FTD	Failure to Detect / Fallo a Detectar
FTP	Failure to Process / Fallo a Procesar
FPS	Frames Per Second / Fotogramas Por Segundo
CMC	Cumulative Match Characteristic / Característica de Emparejamiento Acumulativa
IQS	Image Quality Specification / Especificación de Calidad de Imagen
EFTS	Electronic Fingerprint Transmission Specification / Especificación para Transmisión Electrónica de Huellas Dactilares

PPI	Pixels Per Inch / Píxeles Por Pulgada
ISO	International Organization for Standarization / Organización Internacional de Normalización
CC	Common Criteria / Criterio común
IEC	International Electrotechnical Commission / Comisión Electrotécnica Internacional
UE	Unión Europea
DNI	Documento Nacional de Identidad
BBDD	Bases de Datos
DNIe	Documento Nacional de Identidad electrónico
NIST	National Institute of Standards and Technology / Instituto Nacional de Estándares y Tecnología
TOE	Target Of Evaluation / Objetivo De Evaluación
PIN	Personal Identification Number / Número de Identificación Personal
PCD	Puesto de Control Desatendido
PCA	Puesto de Control Atendido
PC	Personal Computer / Ordenador Personal
SAI	Sistema de Alimentación Ininterrumpido
UPS	Uninterrumpible Power Supply / Sistema de Alimentación Ininterrumpido
CNP	Cuerpo Nacional de Policía
UV	Ultravioleta
IR	Infrarrojo
ICAO	International Civil Aviation Organization / Organización de Aviación Civil Internacional

EPIS	Sistema de Inspección de Pasaportes
MoC	Match on Card / Comparación en Tarjeta
LED	Light Emitting Diode / Diodo Emisor de Luz
3D	Tres Dimensiones
SoC	Storage on Card / Almacenamiento en Tarjeta
TAR	True Acceptance Rate / Tasa de Verdadera Aceptación

1 Introducción

1.1 Motivación y objetivos

A partir de los años 60 se comenzaron a desarrollar los primeros sistemas automáticos de identificación basados en técnicas biométricas. Estas técnicas de reconocimiento tenían un gran interés porque suponían una forma segura y sencilla de identificar a personas; lo que hacía posible abandonar los sistemas tradicionales que conllevaban riesgos de seguridad importantes (tarjetas de identificación y/o contraseñas que podían ser perdidas, olvidadas o sustraídas). Por ello, los sistemas biométricos han experimentado un enorme crecimiento y actualmente están presentes en multitud de escenarios: control de pasajeros en aeropuertos, autenticación de documentos, Smartphone, control de acceso a zonas restringidas, control de asistencia laboral, etc.

Los sistemas de reconocimiento biométrico usan rasgos biométricos propios de cada individuo para identificarlo, es decir, que se reconoce al usuario por lo que es en lugar de por lo que tiene o sabe. De esta forma, el objetivo será obtener, a partir de la captura de un rasgo biométrico, una representación de cada individuo que resulte lo suficientemente discriminante respecto a las de los demás usuarios del sistema; de modo que el sistema sea capaz de determinar la identidad del usuario que está intentando acceder al sistema o simplemente si el usuario está registrado o no en él, dependiendo del tipo de aplicación para la que se utilice.

Sin embargo, a pesar de que los sistemas biométricos están siendo usados cada vez más, no es una práctica común la evaluación de los sistemas de identificación para que cumplan ciertos requisitos de rendimiento y/o de seguridad. Esto se debe a que evaluar un sistema biométrico es un reto muy difícil. El análisis de cualquier característica en este tipo de sistemas requiere controlar muchos factores lo cual conlleva un proceso muy complejo.

Actualmente la información referente a la evaluación de estos sistemas se encuentra dispersa en muchos documentos. La motivación de este TFG es utilizar todas esas metodologías dispersas, reunirlas, desarrollarlas y complementarlas para definir una metodología general para la evaluación de la seguridad de un sistema biométrico.

También serán objeto de estudio los sistemas automáticos de control de fronteras (sistemas ABC). Dichos sistemas controlan los accesos y cruces fronterizos de forma automatizada en una gran cantidad de aeropuertos del mundo. Puesto que dichos sistemas son muy importantes para evitar inmigración ilegal o problemas de seguridad nacional, se analizarán las vulnerabilidades de los sistemas ABC aplicando la metodología para la evaluación de la seguridad desarrollada y añadiendo nuevos aspectos característicos del control de fronteras.

Por lo tanto, el objetivo de este TFG es generar una guía para la evaluación de la seguridad de los sistemas biométricos y validarlo, aplicándolo a los sistemas automáticos de control de fronteras (ABC).

1.2 Entorno socio-económico y marco regulador

En muy poco tiempo, los sistemas biométricos se han vuelto indispensables en los escenarios donde el reconocimiento de una identidad y la seguridad son factores importantes como puede ser en un control de fronteras o en un banco. Sin embargo, a pesar de que estos sistemas están siendo usados cada vez más, la evaluación de los sistemas de identificación para que cumplan ciertos requisitos de rendimiento y/o de seguridad, no es una práctica común. Esto se debe a que evaluar un sistema biométrico es un reto muy difícil. El análisis de cualquier característica en este tipo de sistemas requiere controlar muchos factores lo cual conlleva un proceso muy complejo.

Este vacío en la evaluación fue en parte resuelto por la publicación del estándar ISO/IEC 19795 Biometric performance testing and reporting [1]. Este estándar establece los principios básicos del rendimiento en pruebas y define un entorno de trabajo para planear, ejecutar y reportar cualquier tipo de evaluación.

No obstante, no incluye ninguna evaluación para la seguridad de un sistema. Posteriormente en la literatura, se han publicado diferentes documentos relacionados con la seguridad. Por ejemplo, hay documentos que describen las amenazas de un sistema biométrico (ejemplo: BEM [2]) o de diferentes ataques (ejemplo: ISO/IEC 19792 standard [3]), metodologías que definen como calcular el potencial de ataque o la probabilidad de que un ataque tenga éxito como el Biometric Institute Framework [4] o Common Criteria [5] para cualquier tipo de identificación, y otros documentos que proponen medidas para cuantificar el nivel de seguridad alcanzado frente a amenazas como el European Project Tabula Rasa [6]. Sin embargo, ninguno de estos documentos establece una metodología completa que evalúe el sistema de forma global.

Los desarrolladores y laboratorios de testeo siguen necesitando la definición de este proceso de evaluación para ayudarles a evaluar sistemas biométricos. Además, muchos de los documentos mencionados no consideran el sistema completo o sus medidas, lo cual es indispensable para descartar aquellos ataques que no son viables y como consecuencia, reducir y simplificar la evaluación.

En este TFG, se define una metodología general para la evaluación de la seguridad de un sistema biométrico basada en todos los documentos existentes anteriormente mencionados y complementada con otros aspectos que hasta el momento, no habían sido tratados.

1.3 Estructura del documento

Este documento se escribe en diversos capítulos, cada uno de ellos encargado de facilitar la información pertinente de cada elemento a tener en cuenta en la realización de este TFG:

- Capítulo 1: El presente capítulo, es el capítulo introductorio de la memoria, el cual inicia al lector de esta. Se incluyen las motivaciones y los objetivos que han llevado a realizar este Trabajo de Fin de Grado.

- Capítulo 2: En este capítulo, se analizará la evolución de la biometría y los sistemas de reconocimiento para reflejar importancia de la evaluación de la seguridad.

- Capítulo 3: Se definirá una metodología general para la evaluación de la seguridad de cualquier sistema biométrico. Dicho capítulo está basado en los documentos previos desarrollados sobre el tema y/o en metodologías similares para otras tecnologías ya existentes.
- Capítulo 4: Una vez se han definido requisitos y los procedimientos que se deben evaluar para cualquier sistema biométrico entonces se aplicará dicha metodología para un sistema ABC. En particular y debido a que para muchos apartados se necesita información específica se usará como ejemplo los sistemas ABC españoles implantados en los aeropuertos nacionales.
- Capítulo 5: Un último capítulo a modo de conclusión sobre el trabajo realizado y sobre futuras líneas de investigación en torno a la metodología de evaluación.

Adicionalmente, se presenta un capítulo con la bibliografía y un anexo con información referente a la planificación y al presupuesto del TFG.

2 Estado del arte

La biometría es la ciencia que estudia el reconocimiento de seres humanos de forma automática, utilizando para tal fin una o varias características fisiológicas o de comportamiento que resulten lo suficientemente discriminativas dentro de una población. El término "biometría" proviene de las palabras griegas "bios" (vida) y "metrón" (medida).

2.1 Características de los rasgos biométricos

Las características en las que se basa un sistema de reconocimiento biométrico son conocidas como rasgos biométricos. Estos rasgos se dividen en una posible clasificación:

- Rasgos fisiológicos: Presentan una variabilidad reducida a lo largo del tiempo pero su adquisición requiere de la cooperación de los usuarios y es más invasiva. El iris, la huella dactilar o la geometría de la mano pertenecen a este grupo.

- Rasgos conductuales o de comportamiento: Resultan menos invasivos pero presentan una gran variabilidad (factores como el estado anímico, el cansancio o estrés pueden influir en rasgo biométrico) por lo que, la exactitud de los sistemas basados en este tipo de rasgos será menor. La voz, la escritura o la forma de andar pertenecen a este grupo.

Además, para que el rasgo biométrico pueda ser utilizado como base de un sistema de reconocimiento, debe cumplir siete requisitos básicos [7] :

1. **Universalidad:** Que esté presente en todas las personas.

2. **Unicidad:** Que sea diferente para cada individuo.

3. **Permanencia:** Que permanece invariante a lo largo del tiempo.

4. **Mensurabilidad:** Que pueda ser capturado y medido fácilmente mediante un proceso de adquisición.

5. **Rendimiento:** Que pueda dar lugar a un sistema de reconocimiento con baja tasa de error, alta velocidad y mínimo consumo de recursos.

6. **Aceptabilidad:** Que cuenta con un alto grado de aceptación social.

7. **Evitabilidad:** Que es difícilmente eludible mediante procedimientos fraudulentos y como resultado sistemas seguros.

Sin embargo, no existe ningún rasgo biométrico conocido que cumpla completamente todos estos requisitos; por lo que la elección del mismo, se basará en las características propias de la aplicación en la que vaya a ser utilizado (ver Figura 1).

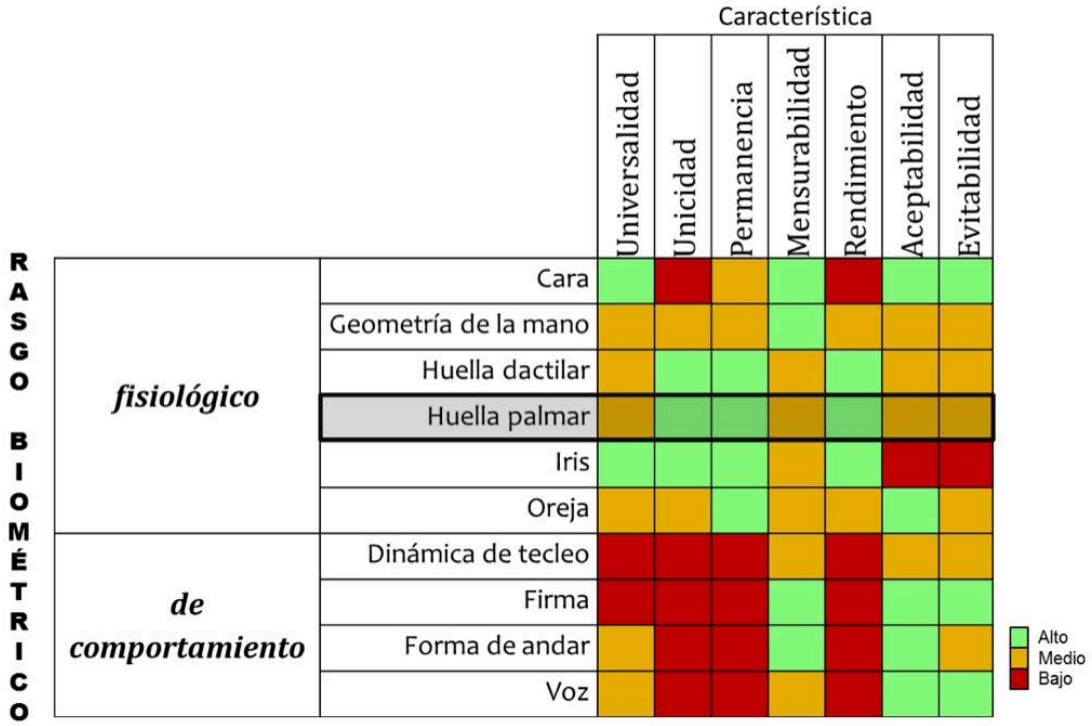
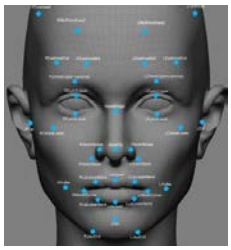


Figura 1. Comparativa entre las características de distintos rasgos biométricos [7]

2.2 Tipos de rasgos biométricos

Existen numerosos rasgos biométricos que son objeto de estudio, algunos de los más habituales se resumen a continuación.

- **Fisiológicos**



Cara. La cara es el rasgo biométrico que un ser humano utiliza de forma natural para reconocer a otra persona y por ello cuenta con una fuerte aceptación social. Además su adquisición no resulta invasiva, puede hacerse a distancia y sin cooperación por parte del usuario. Como se vio en la figura 1 el sistema de reconocimiento facial genera peor rendimiento que otros rasgos biométricos. Esto se debe a que necesita de unas condiciones ambientales específicas para conseguir un rendimiento aceptable.

Geometría de la mano. La adquisición de una imagen de la mano puede realizarse por medio de un sencillo escáner. Una vez obtenido el contorno de la mano, se extraen una serie de medidas distintivas (como la longitud y grosor de los dedos, el tamaño de la palma, el perímetro, etc.). Los sistemas basados en este rasgo proporcionan buenos resultados en poblaciones de pequeño/mediano tamaño.

Huella dactilar. Una huella dactilar está compuesta por un conjunto de valles y crestas. Su alto grado de unicidad y su permanencia en el tiempo ha posibilitado que haya sido uno de los rasgos más estudiados y extendidos. El reconocimiento dactilar se propuso desde finales del siglo XIX dentro del ámbito forense, y desde entonces ha avanzado enormemente en ese campo pero actualmente también puede encontrarse en numerosas aplicaciones comerciales.

Huella palmar. La huella palmar está formada por un patrón de crestas y valles de la misma forma que la huella dactilar pero en toda la superficie de la palma, además de contener un conjunto de líneas principales. El área de una huella palmar es mucho mayor que el de una huella dactilar, resultando un rasgo altamente distintivo; pero, por otro lado, es necesario un sensor de mayores dimensiones. Tras el éxito de los sistemas de reconocimiento dactilar, la huella palmar ha suscitado un creciente interés en los últimos años.

Iris. Situado detrás de la córnea, el iris es una membrana circular y cuya textura permanece invariante a lo largo del tiempo y es única para cada individuo. Se trata de uno de los rasgos más distintivos, por lo que ha sido utilizado en aplicaciones de alta seguridad. Sin embargo, la adquisición del iris necesita sensores que resultan demasiado costosos para determinadas aplicaciones y requiere de un alto grado de cooperación de los usuarios, que deben posicionarse a una muy corta distancia del sensor para su captura.

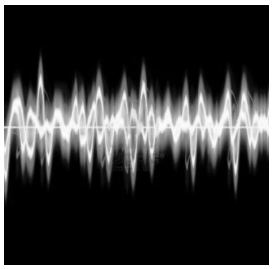
Oreja. El reconocimiento basado en la forma de la oreja suele realizarse mediante la selección de un punto de referencia en el interior de la misma y la distancia de éste a puntos característicos que forman el borde de la oreja y sus estructuras cartilaginosas. A diferencia de la cara, la oreja se mantiene invariante con el paso del tiempo, no cambia su forma con la expresión y es menos sensible a cambios de iluminación. Un inconveniente es que puede estar oculta tras el pelo; donde se plantea como solución realizar la captura en la banda de infrarrojos.

- **De comportamiento**

Dinámica del tecleo. Debido a que cada persona interacciona con el teclado de forma distinta, los sistemas de identificación basados en dinámica del tecleo pueden presentar una solución en casos sencillos de acceso a aplicaciones on-line. Sin embargo, se trata de un rasgo biométrico de baja unicidad y alta variabilidad, pero cuya adquisición no resulta invasiva.

Firma. Ha sido tradicionalmente usada como medio de autentificación y es el sistema de reconocimiento más aceptado. Su adquisición no resulta invasiva aunque requiere de la cooperación del sujeto. La forma con la que se firma caracteriza a cada persona; sin embargo, presenta alta variabilidad. La aparición de dispositivos móviles con interfaz tipo puntero, dio lugar al reconocimiento basado en firma manuscrita dinámica donde, además de la forma, se utiliza información instantánea (como la duración de la misma, la velocidad o la presión) logrando implementar sistemas de reconocimiento con elevada tasa de acierto.

Forma de andar. Cada persona camina de forma diferente. Aunque este rasgo presenta baja unicidad y consigue tasas de acierto menores que otros rasgos de comportamiento, resulta una solución útil cuando se quiere identificar a un sujeto en una secuencia de vídeo (por ejemplo a un criminal en una grabación de una cámara de seguridad).



Voz. La señal de voz codifica mediante sonidos, llamados alófonos. Las distintas configuraciones del tracto vocal producen distintos sonidos. Al ser único el tracto vocal de cada persona, la señal de voz presenta características físicas invariantes que resultan suficientemente distintivas. En este sentido, podría clasificarse como un rasgo fisiológico. Sin embargo, la señal de voz resultante también está influenciada por otros factores de comportamiento (como el estado emocional, patologías o la edad) que no permanecen estables en el tiempo y dificultan la tarea de reconocimiento. Aun así, la voz es un rasgo biométrico ampliamente aceptado y juega un papel importante en aplicaciones telefónicas.

2.3 Sistemas biométricos

Un sistema biométrico permite determinar o verificar automáticamente la identidad de un individuo mediante técnicas de reconocimiento de patrones.

El primer paso para llevar a cabo la identificación/verificación del sujeto que se enfrenta al sistema biométrico consiste en la adquisición de su rasgo biométrico mediante un transductor que digitaliza el rasgo capturado. La calidad del mismo será de vital importancia puesto que repercute en todas las etapas sucesivas, y por tanto en el rendimiento total del sistema. Por este motivo, la captura requiere en algunas ocasiones de la cooperación del usuario, e incluso puede estar supervisada.

Tras un acondicionamiento, se realiza un modelo de usuario a partir de una serie de características o parámetros que el sistema biométrico considera discriminante en la señal pre procesada. Este modelo de usuario es comparado con otro proveniente de una base de datos, generándose una puntuación que indicará la similitud entre ambos modelos. A partir de esta puntuación, se decide (en general mediante un umbral que el sistema tiene prefijado) si el modelo almacenado en la base de datos coincide o no con el del usuario en cuestión. La Figura 2 esquematiza las etapas básicas de un sistema biométrico como el que se ha descrito.

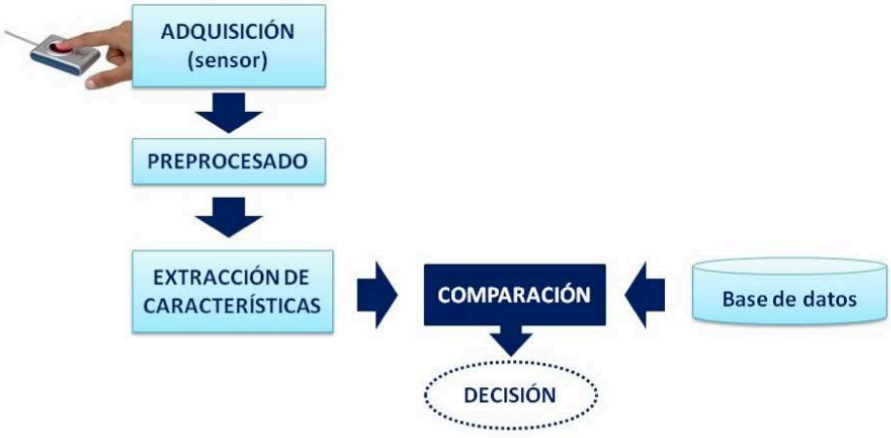


Figura 2. Funcionamiento básico de un sistema biométrico.

La base de datos del sistema biométrico que contiene todos los modelos de usuario se debe realizar con anterioridad. Es un proceso que se denomina reclutamiento. El reclutamiento de cada usuario tiene por objeto construir un modelo que lo caracterice, siendo necesario poseer una o varias capturas del rasgo biométrico del usuario.

2.3.1 Sistemas multi biométricos

En un sistema biométrico es posible reducir el margen error pero existen ciertas limitaciones que no pueden evitarse. La variabilidad, la calidad en las muestras adquiridas o los posibles ataques a los sistemas son algunos ejemplos. En este sentido, la multi biometría se plantea como una buena opción para reducir el margen de error y aumentar la seguridad frente a ataques creando un sistema mucho más seguro.

Los sistemas multi biométricos hacen uso de más de una fuente de información para realizar la tarea de reconocimiento; pudiendo utilizar, según el escenario: múltiples sensores, rasgos biométricos, instancias (como huellas de varios dedos de una persona), capturas (como una secuencia de imágenes del iris) o representaciones de un mismo rasgo biométrico (como distintos métodos de extracción o comparación de características). Algunas de sus ventajas frente a los sistemas que analizan un solo rasgo son:

- Pueden ser utilizados por un mayor porcentaje de población.
- Resultan más seguros frente a ataques.
- Alcanzan mayores niveles de precisión al combinar la información distintas fuentes.

Los sistemas multi biométricos además pueden operar en modo serie si la salida del análisis de una fuente se toma como entrada de la siguiente; o en modo paralelo si la información de las distintas fuentes se emplea de forma simultánea en el proceso de reconocimiento. Además, el módulo de fusión que combina la información de los distintos sistemas puede situarse: a nivel de extracción de características, a nivel de score o a nivel de decisión.

2.4 Aplicaciones de los sistemas biométricos

Las características y requisitos propios de cada sistema biométrico dependen directamente de la aplicación para la que vayan a ser utilizados. Tradicionalmente se distinguen tres campos de aplicación: comercial, gubernamental y forense. Sin embargo, esta división no aporta una idea de las características de los sistemas en cada tipo de aplicación; pudiendo dentro de un mismo campo coexistir sistemas con requisitos y necesidades completamente distintas.

Es posible hacer otra clasificación partiendo de criterios como: la forma en que el usuario interacciona con el sistema, los requisitos de rendimiento, el grado de cooperación de los usuarios, el modo de operación del sistema, etc. Esto nos proporciona una segunda clasificación que los divide en las siguientes categorías [8]: identificación criminal, terminales en puntos de venta, comercio electrónico, acceso a dispositivos personales, acceso físico a zonas restringidas, verificación de identidad del ciudadano y servicios de vigilancia.

Como se puede observar las posibles aplicaciones de los sistemas biométricos son múltiples y muy diferentes. Por ello, en los últimos años el uso de los sistemas biométricos se ha incrementado enormemente. Ejemplo de ello y dada la importancia para el desarrollo del TFG se hará una breve introducción a los sistemas ABC.

2.4.1 Sistemas ABC

Un sistema ABC (también conocido como e-Gate) se define como el uso automatizado y semi-automatizado que puede verificar la identidad de viajeros a través de fronteras sin la necesidad de intervención humana. Actualmente, los sistemas ABC se basan en el uso de un documento electrónico de viaje que contiene las muestras biométricas para realizar la verificación, suelen incluir imágenes de la cara y la huella dactilar del dueño del documento de viaje.

Figura 3. Ejemplo de sistema ABC

El proceso automático en el control de fronteras empieza con el escaneado del pasaporte electrónico introduciendo la parte del pasaporte con la información personal en el lector. Dicho lector realiza ciertas comprobaciones de seguridad y se comunica con el chip para identificar la autenticidad del documento. Después, se captura una imagen de la cara del viajero y se compara con la que hay almacenada en el chip. Aquí también se hace la comprobación de otro rasgo biométrico dependiendo de la configuración del sistema ABC que se haya implementado. Si la verificación ha sido satisfactoria entonces la e-Gate deja al pasajero finalizar el cruce fronterizo y sino, el viajero es reconducido al control de fronteras manual. Durante todo este proceso hay una supervisión humana que además puede realizar comprobaciones adicionales como cotejar identidades en bases de datos.

El objetivo de los sistemas ABC es por un lado facilitar el reconocimiento, aumentar la seguridad y automatizar el control de fronteras para personas de la UE, Islandia, Noruega y Suiza, mayor de 18 años y con pasaporte o DNI electrónico. Y por otro lado reducir los costes para dicho control puesto que un sistema ABC exige menos personal que el sistema tradicional.

2.4.1.1 Principales funciones y características

Los sistemas ABC realizan las siguientes tareas con un alto nivel de automatización:

- Comprobar que el viajero que intenta cruzar la frontera utiliza un documento de viaje válido y original. Lo que se conoce por verificación documental.
- Comprobar biométricamente que ese documento de viaje pertenece al viajero que está intentando cruzar la frontera. Lo que se conoce por proceso de verificación.
- Comprobar que el viajero está autorizado para cruzar la frontera.
- Permitir o no el cruce fronterizo de acuerdo a una lógica predefinida aunque algunas veces requiera la asistencia externa para realizar todo el proceso de comprobación.
- Garantiza la seguridad del proceso completo por lo que sólo un viajero que claramente haya pasado todas las comprobaciones se le permitirá el cruce de la frontera. Para cualquier fallo en las comprobaciones y se le reconducirá a un puesto asistido por humanos que supervisarán más de cerca el proceso.

Estas son las características básicas que todo sistema ABC debe tener aunque existen comprobaciones adicionales que dependen de la configuración del sistema como se verá más adelante. Como mínimo incluirán:

- Barreras físicas (una o dos e-Gates)
- Lector de pasaportes electrónicos: Reconocimiento óptico de la página biográfica y una lector de radio frecuencia (RF) para comunicarse con el chip.
- Monitor para mostrar las instrucciones.
- Sensor biométrico.
- Sistema que gestiones el hardware y el software.

Como se verá más adelante en la metodología de evaluación de los sistemas automático de control de fronteras (capítulo 4) se analizará en profundidad un sistema ABC español, que incluye otros sistemas de comprobación adicionales a los básicos.

2.5 Modos de funcionamiento de un sistema biométrico

Una vez se ha realizado el reclutamiento de varios usuarios (esto es, existe al menos un modelo de cada uno de ellos), un sistema biométrico puede operar en los siguientes modos:

- Verificación: El usuario que se enfrenta al sistema de reconocimiento presenta su rasgo biométrico y proporciona su identificador de usuario. Posteriormente, se busca en la base de datos el modelo de usuario correspondiente a dicho identificador y se compara con el creado a partir de la realización actual. Es lo que se denomina reconocimiento positivo y requiere de una comparación uno a uno (1-1). Con la puntuación de salida de la comparación, y a partir de un umbral, el sistema toma una decisión: se trata de un usuario genuino si es quien dice ser o bien de un usuario impostor.

- Identificación: El sistema intenta determinar si el usuario, del que se ha capturado el rasgo biométrico, se encuentra en la base de datos, para lo cual se realiza una comparación contra todos los modelos de los usuarios registrados. Se trata de una comparación uno a muchos (1-N). Como resultado se genera una lista de candidatos cuyas puntuaciones están ordenadas de mayor a menor; a menos que ninguna de las puntuaciones obtenidas haya alcanzado un umbral de similitud con el que se pueda afirmar que el usuario se encuentra registrado.

  El modo de identificación requiere un coste computacional mucho más elevado que el modo de verificación. Por ello, es habitual que su uso se limite a aplicaciones en las que el usuario no quiera ser reconocido. En este caso se trata de reconocimiento negativo y únicamente puede realizarse mediante sistemas biométricos.

Adicionalmente los modos de verificación e identificación pueden implementarse en sistemas online u offline. Los sistemas online capturan el rasgo biométrico y lo procesan en tiempo real; de esta forma, la velocidad será su requisito principal. Por otro lado, los sistemas offline trabajan con rasgos biométricos que ya han sido capturados previamente, y buscarán minimizar la tasa de error a costa de incrementar el tiempo de procesamiento.

La aplicación para la que vaya a ser utilizado determina el tipo de sistema biométrico y su configuración. Por ejemplo, se usan sistemas online en controles de acceso y sistemas offline para la identificación de criminales a partir de pruebas, como huellas, en el escenario de un crimen.

2.6 Evaluación de un sistema biométrico

La evaluación de un sistema biométrico como se dijo anteriormente, no es una tarea sencilla ya que requiere controlar muchas variables. A pesar de ello, existen factores presentes en todo sistema biométrico:

- Evaluación de conformidad: Determina si se cumplen determinados requisitos previamente definidos.
- Evaluación de seguridad: Determina si se cumplen unos niveles de seguridad predeterminados. También se analizan vulnerabilidades del sistema.
- Evaluación de usabilidad y aceptabilidad: Se determina desde el punto de visa del usuario.
- Evaluación de rendimiento: Determina la rapidez y precisión con la que el sistema realiza el proceso de reclutamiento y reconocimiento. Se basa en parámetros estadísticos.

Pese a que estos y otros factores pueden evaluarse sólo se van a comentar los más relevantes para este TFG: el rendimiento y la seguridad.

2.6.1 Evaluación del rendimiento

Para implementar un sistema automático de reconocimiento se necesitan mecanismos que evalúen el rendimiento y/o la capacidad del sistema. Cuantificar el error que produce el sistema ayudará a su desarrollador a mejorarlo y a compararlo con otros ya implementados.

Un sistema de reconocimiento captura un rasgo biométrico, extrae sus características y forma un modelo que compara con otro u otros para evaluar si pertenecen o no a una misma persona. De esta forma, se requiere que rasgos biométricos de distintas personas sean muy distintos y que modelos generados a partir del rasgo biométrico de una misma persona sean muy parecidos. Sin embargo, existen factores que dan lugar a errores en el reconocimiento. Por ejemplo, un usuario que interactúe con el sensor de forma distinta o que experimente cambios de comportamiento o fisiológicos, puede hacer que el sistema genere modelos muy distintos a partir de un mismo rasgo biométrico.

La salida de un sistema de reconocimiento es generalmente una puntuación o score, fruto de la comparación de dos modelos, que cuantifica el grado de similitud entre los mismos. A partir de estas puntuaciones, se establece un umbral con el que el sistema decide si el usuario es genuino (si el score supera el umbral) o impostor (en caso contrario). Esta decisión da lugar a que se puedan cometer dos tipos de errores:

- El sistema detecta un usuario como impostor siendo en realidad un usuario genuino. Esto ocurre cuando dos modelos pertenecientes a un mismo usuario generan una puntuación por debajo del umbral de similitud. Es lo que se denomina Tasa de falso rechazo o False Reject Rate (FRR).

- El sistema detecta un usuario como genuino siendo en realidad un usuario impostor. Es decir, dos modelos pertenecientes a distintos usuarios generan una puntuación por encima del umbral de similitud. Es lo que se denomina falsa aceptación y se evalúa con la Tasa de Falsa Aceptación o False Accept Rate (FAR).

El análisis y tratamiento de los errores se enfoca de forma distinta según el modo de funcionamiento. Por eso, se analizará el rendimiento para el modo de verificación y modo de identificación.

2.6.1.1 Evaluación del rendimiento de sistemas biométricos en modo de verificación

Como se introducía anteriormente se usará la FAR y FRR. En la Figura 4 aparecen ambas tasas para cada puntuación o score. La tasa de FAR siempre decrece frente a la puntuación puesto que a medida que disminuye el umbral más probabilidad hay de que el sistema acepte a un usuario impostor. Por el contrario, la FRR será creciente con el umbral ya que a mayor umbral, mayor posibilidad existe de rechazar a un usuario válido.

En un sistema ideal, las curvas FAR y FRR quedarían completamente separadas por el umbral escogido; pero en los sistemas reales ambas curvas se superponen, asumiendo siempre un error de falsa aceptación y otro de falso rechazo, que nunca podrán disminuir al mismo tiempo. El punto donde ambas tasas se igualan, FAR=FRR, se conoce como EER (Equal Error Rate) y puede utilizarse como referencia para comparar distintos sistemas. Sin embargo, es poco habitual que el punto de trabajo coincida con el EER, ya que el umbral se escoge en función del tipo de aplicación para la que se desarrolle el sistema. Por ejemplo, se utilizan umbrales bajos en algunas aplicaciones comerciales con el fin de que la tasa de falso rechazo

disminuya y no resulte molesta para los usuarios y umbrales altos en aplicaciones de alta seguridad, disminuyendo la probabilidad de que un usuario impostor sea aceptado por el sistema; a costa de incrementar la probabilidad de que un usuario genuino sea rechazado.

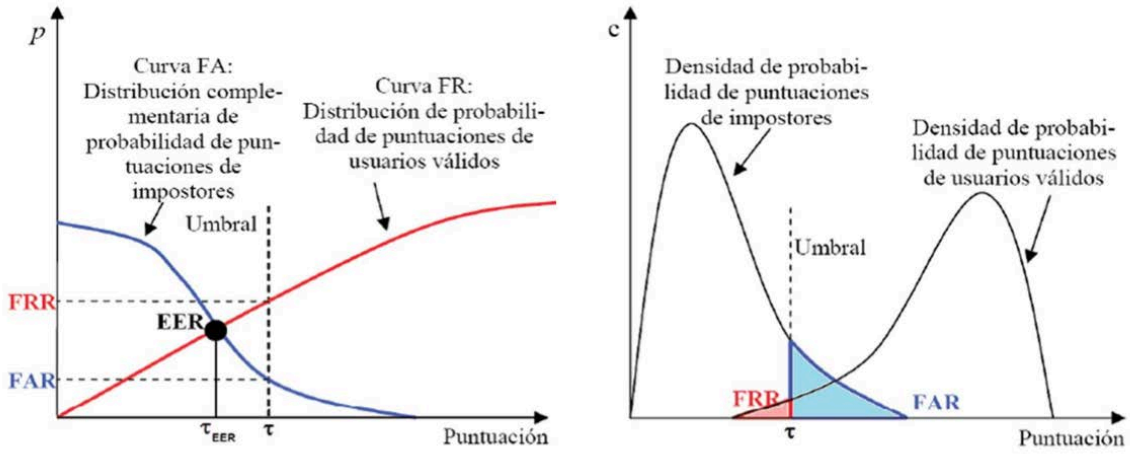


Figura 4. Distribución y densidad de probabilidad de usuarios genuinos e impostores

También es habitual representar la densidad de probabilidad de las puntuaciones para usuarios genuinos e impostores, como aparece en la Figura 4. Fijado un umbral, el área bajo la curva de impostores que quede por encima del mismo, coincide con la probabilidad de que un impostor sea aceptado (FAR); así como el área bajo la curva de usuarios genuinos por debajo del umbral, coincide con la probabilidad de que el sistema rechace a un usuario válido (FRR).

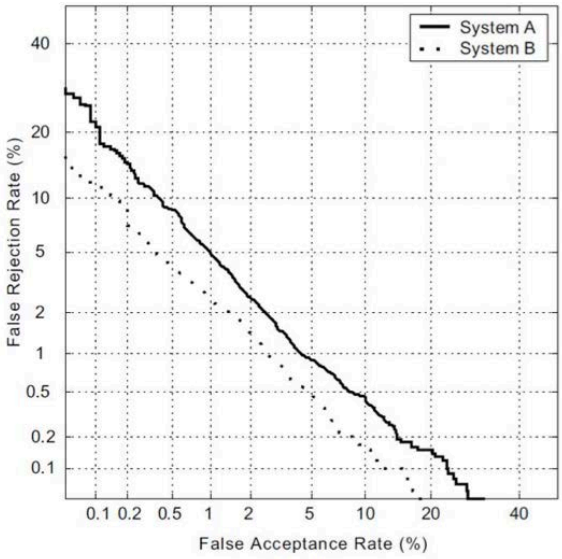


Figura 5. Gráfico Receiver Operation Characteristic (ROC)

En algunas ocasiones, el punto de trabajo se fija estableciendo unos límites máximos de error de FAR y FRR. La representación en forma de curvas Receiver Operation Characteristic (ROC) pues resulta muy útil en estos casos. En una curva ROC se presenta un error frente a otro en un eje normalizado, originándose una única curva definida para todos los posibles puntos de trabajo del sistema (ver Figura 5). El EER coincide con el punto donde la curva ROC corta con la bisectriz de la gráfica. Una gran ventaja de este tipo de representación es que permite comparar a simple vista distintos tipos de sistemas en cualquier punto de trabajo. Cuanto mejor sea el sistema, más se acercará su curva ROC al origen (menor porcentaje de errores FAR y FRR).

2.6.1.2 Evaluación del rendimiento de sistemas biométricos en modo de identificación

Como se definió anteriormente, cuando un sistema biométrico que trabaja en modo de identificación hace una comparación uno a muchos (1-N) y devuelve el modelo que mayor puntuación haya obtenido. En este caso, se mide la frecuencia con la que el modelo del usuario genuino consigue la mayor puntuación. Otras veces el sistema devuelve una lista de N candidatos que superan un cierto nivel de similitud, y se trabaja con curvas Cumulative Match Characteristic (CMC) como la de la Figura 6. Estas curvas indican la probabilidad con la que el candidato genuino aparece en cada posición de la lista devuelta por el sistema.

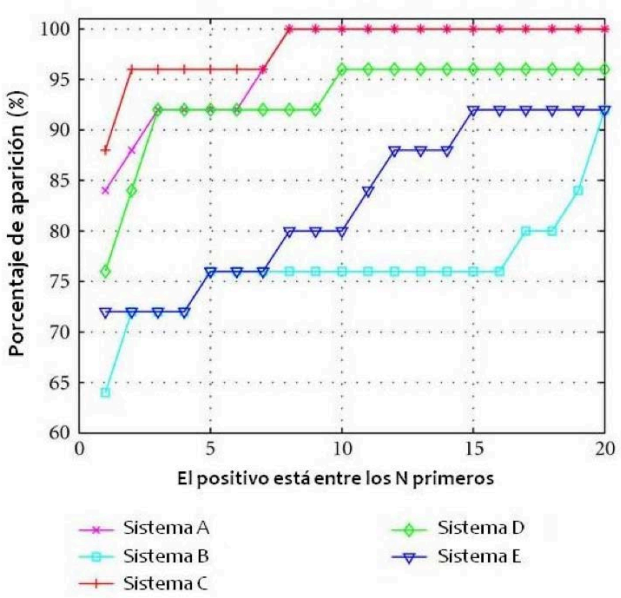


Figura 6. Ejemplo de CMC

2.6.2 Evaluación de la seguridad

Como se explicó anteriormente la evaluación de seguridad aún no tiene unos estándares. Existen documentos que han ido cubriendo los vacíos en relación a las metodologías de evaluación de los sistemas biométricos como es el caso del estándar ISO/IEC 19795 Biometric Performance testing and reporting [1]. Este estándar establece los principios básicos del rendimiento en pruebas y define un entorno de trabajo para planear, ejecutar y reportar cualquier tipo de evaluación.

Posteriormente en la literatura, se han publicado diferentes documentos relacionados con la evaluación de la seguridad. Por ejemplo, hay documentos que describen las amenazas de un sistema biométrico (ejemplo: BEM [2]) o de diferentes ataques (ejemplo: ISO/IEC 19792 standard [3]), metodologías que definen como calcular el potencial de ataque o la probabilidad de que un ataque tenga éxito como el Biometric Institute Framework [4] o Common Criteria [5] para cualquier tipo de identificación, y otros documentos que proponen medidas para cuantificar el nivel de seguridad alcanzado frente a amenazas como el European Project Tabula Rasa [6]. Sin embargo, ninguno de estos documentos establece una metodología completa que evalúe el sistema de forma global.

Puesto que la metodología de evaluación de la seguridad no es completa este TFG tiene por objetivo el desarrollo de dicha metodología cubriendo todos los factores anteriormente comentados. Dicha metodología se describe detalladamente en el capítulo 3.

2.7 Aceptación social y privacidad

La privacidad es un punto fundamental y ampliamente cuestionado al hacer uso de un sistema biométrico. El apoyo de la sociedad es un requisito básico cuando se desea implantar un nuevo sistema. El grado de aceptación social depende en gran medida de la facilidad y comodidad con la que se interaccione con el sistema; cuanto menor cooperación se necesite del usuario, más cómodo resulta y mayor aceptación tendrá. Por otro lado, el hecho de que se pueda captar un rasgo biométrico sin cooperación de los usuarios, se percibe como una amenaza a la privacidad de las personas. El acceso a los rasgos biométricos no sólo reduce el anonimato, sino que puede proporcionar información muy personal (edad, género, afecciones médicas, discapacidades, etc.). Por contra, los defensores de los sistemas biométricos afirman que éstos pueden utilizarse como [7]:

- Protección de la privacidad individual: Por ejemplo, el acceso a un servicio basado en claves o contraseñas es vulnerable ya que pueden ser adivinadas u obtenidas clandestinamente. En este sentido, los sistemas biométricos protegen el acceso a ciertos servicios e información de los usuarios.
- Barrera para el acceso a información personal: Se pueden utilizar sistemas biométricos para restringir directamente el acceso a cierto tipo de información (como informes médicos de pacientes en una base de datos).
- Tecnología de protección de la intimidad: Los sistemas biométricos actuales no almacenan el rasgo biométrico capturado en su forma original, sino que guardan una representación digital en un formato encriptado, impidiendo que la característica física real pueda ser recuperada a partir de su representación digital (encriptación biométrica) .

3 Metodología de evaluación de la seguridad de sistemas biométricos

3.1 Introducción

Cuando se está evaluando la seguridad de un sistema biométrico se deben tener en cuenta diferentes factores ya que permitirán realizar ataques con mayor o menor éxito. Con este documento se pretende analizar de principio a fin una evaluación de seguridad, desde el desarrollo de la idea hasta la ejecución de las pruebas y el análisis de los resultados.

Básicamente el estudio constará de 3 fases: Identificación de posibles vulnerabilidades, estudio y definición de los ataques y por último, fase de penetración o pruebas (ver Figura 7 y 8).

Después, tras concluir la fase de pruebas y calcular la seguridad del sistema se incluye un apartado para redactar un informe acerca de todo el proceso realizado y su posible mejora de la seguridad.

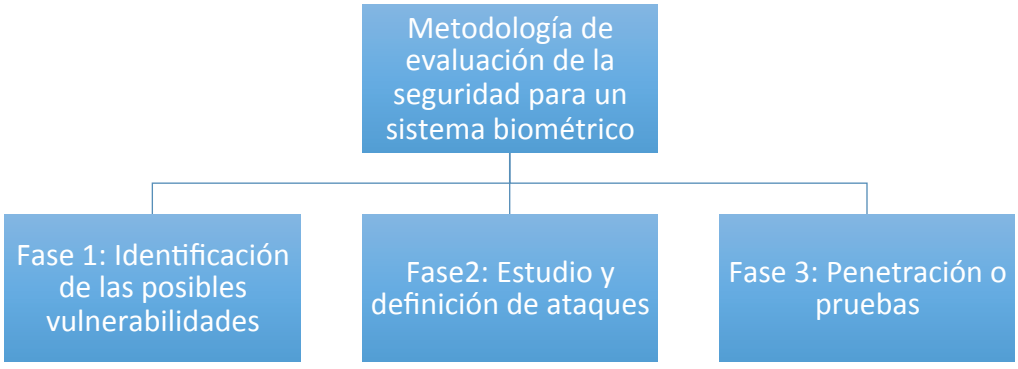


Figura 7. Fases de la metodología de evaluación de la seguridad

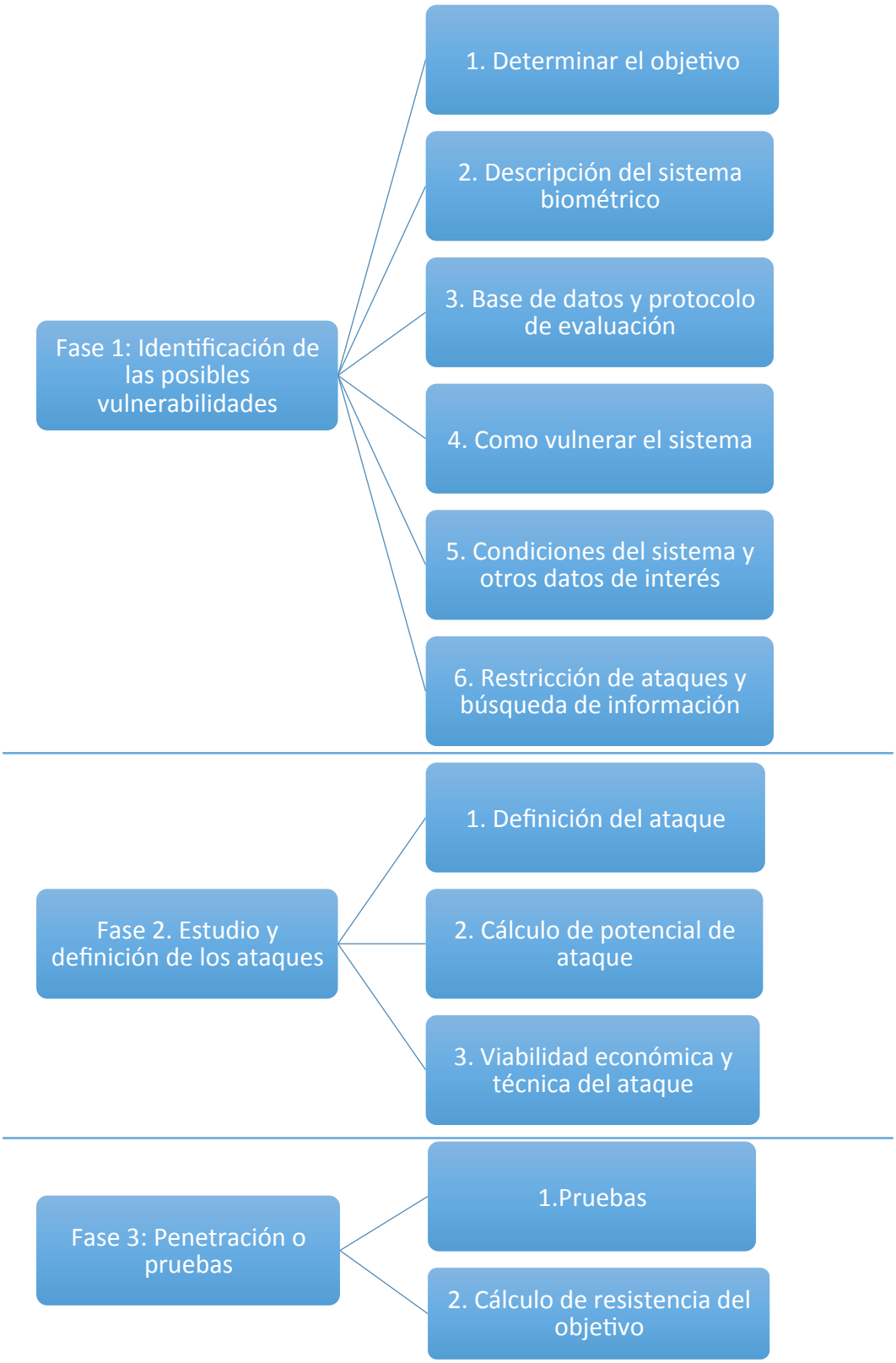


Figura 8. Esquema detallado de las fases de la metodología para la evaluación de la seguridad

3.2 Fase 1: Identificación de posibles vulnerabilidades

En este apartado se debe realizar una descripción del sistema que se someterá a evaluación. Esto incluye su localización, sus condiciones ambientales, qué reconocimiento usa, qué sensores utiliza, etc. En definitiva, las condiciones reales del sistema para restringir la búsqueda de información. Por ejemplo, si pretendemos vulnerar un sistema de identificación dactilar no buscaremos información sobre identificación facial o viceversa. La fase de identificación de las posibles vulnerabilidades y la definición del ataque será el grueso de inversión de tiempo a la hora de evaluar la seguridad de un sistema, por ello se tendrá que restringir la búsqueda de información al sistema bajo evaluación. Muchas veces se encontrarán más vulnerabilidades en los sistemas una vez se esté evaluando otros ataques.

El mundo de la biometría avanza al paso de la tecnología, por lo que es posible que haya factores que no se tengan en cuenta en esta evaluación. Se seguirán los criterios de evaluación de Common Criteria [9] para realizar esta lista.

3.2.1 Determinar el TOE

En primer lugar se deberá identificar cual será el sistema a vulnerar, puesto que sin un objetivo no puede haber un estudio. Puede ir desde lo más simple hasta lo más complejo.

3.2.2 Descripción del sistema

Como evaluador la tarea consistirá en conseguir toda la información posible del sistema referente a su evaluación como sensores, algoritmos, localización, accesibilidad, etc. Para identificar posibles vulnerabilidades y así centralizar la búsqueda de información.

3.2.3 Descripción de las BBDD y arquitectura de evaluación

La base de datos se adquiere mediante el “enrollment” o reclutamiento y asocia una identidad a una muestra biométrica para su posterior uso. Las bases de datos (BBDD) pueden ser centralizadas, conteniendo las muestras en un mismo lugar o bien distribuidas, como puede ser el ejemplo de una tarjeta que contiene los datos para identificar a su portador (DNI e). Una vez se ha reclutado una identidad existen dos formas de reconocimiento:

- **Identificación (Identification):** Comparación de la muestra biométrica que se introduce en el sistema con alguna de la base de datos. Comparación 1-N.
- **Verificación (Verification):** Comparación para demostrar si la muestra biométrica introducida realmente corresponde con la persona que dice ser. Comparación 1-1.

La fase de reclutamiento es muy importante pues será el momento en el que se guarden las muestras biométricas para su posterior uso, ya sea legítimo o ilegítimo. Existen incluso ataques para esta fase como veremos más adelante. En muchos casos la condición física contribuirá a una mejor muestra biométrica.

En todos los casos tanto para el reclutamiento como identificación o verificación hay un procesamiento digital de la muestra biométrica para su almacenamiento o para su comparación.

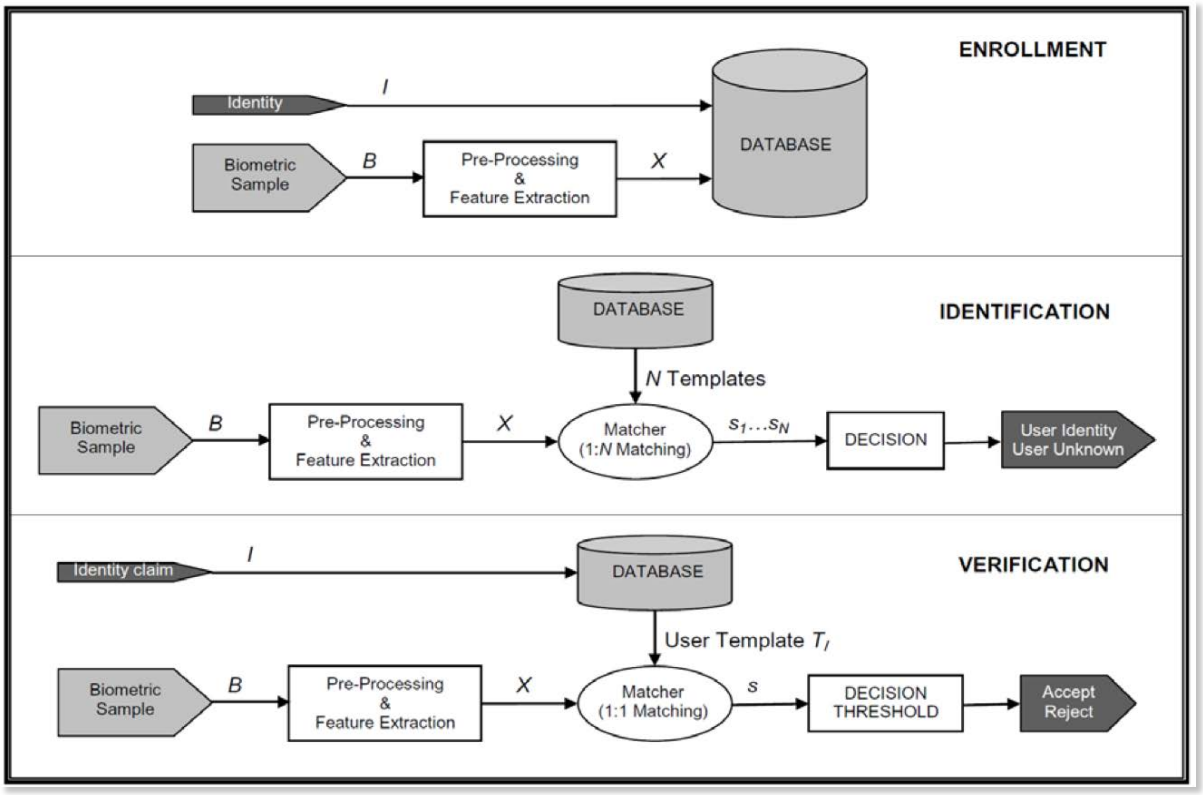


Figura 9. Proceso de reclutamiento, identificación y verificación [9]

3.2.4 Cómo vulnerar el sistema

Existen diferentes modos de vulnerar un sistema, básicamente se incluyen en dos grandes categorías:

- **Identificación (Identification)** corresponde al esfuerzo requerido para crear el ataque y demostrar que puede ser aplicado satisfactoriamente al Target Of Evaluation (TOE) (incluyendo la construcción del equipo necesario). Debe tener en cuenta cualquier dificultad.

- **Explotación (Exploitation)** corresponde a el uso de técnicas o análisis de cierta parte del TOE como parte de un ataque. Varios atacantes pueden ejecutar el ataque y el proceso de explotación puesto que éste ya está definido. Sirve para identificar el posible equipo necesario o herramientas. Muchas veces el potencial de ataque será menor para explotación que para identificación porque tendremos mucha más información. Por ejemplo, si ya sabemos como realizar el ataque y solo queremos explotarlo, no gastaremos tiempo y recursos en identificar la vulnerabilidad.

3.2.5 Rendimiento, fallos u otros datos de interés

Como toda tecnología, tiene sus limitaciones. A la hora de evaluar la seguridad se deberá tener en cuenta factores constructivos o de precisión para hacer una buena evaluación. Para esta labor existen ciertos ratios conocidos en el mundo de la biometría para catalogar la precisión y los buenos resultados de un sistema:

- **FAR (False Accept Rate / Tasa de Falsa Aceptación):** Probabilidad de que un sistema biométrico identifique incorrectamente a un individuo o bien que falle frente a un impostor.
- **FRR (False Reject Rate / Tasa de Falso Rechazo):** Probabilidad de que un sistema falle al identificar o verificar una persona que está ya reclutada en el sistema.
- **ROC (Receiver Operating Characteristic / Característica Operativa del Receptor):** Representación gráfica de la sensibilidad para un sistema clasificador binario según se varía el umbral de discriminación [10].

Tanto la FAR como la FRR o el ROC dará información sobre las limitaciones estadísticas de aceptación falsa o de falso rechazo. Estos datos ayudarán a soportar o descartar ciertos tipos de ataques como se verá más adelante. Si además se pudiera encontrar cualquier otro dato de interés relativo a la condiciones reales como localización, condiciones ambientales de temperatura, humedad, luminosidad, etc. Se podrían encontrar nuevos métodos para vulnerar el sistema o encontrar situaciones en las que el sistema es más propenso a fallar.

3.2.6 Restricción de ataques y búsqueda de información

En base a lo anteriormente redactado se deberá restringir el tipo de ataque o los tipos de ataque que se van a realizar. Siguen el siguiente esquema:

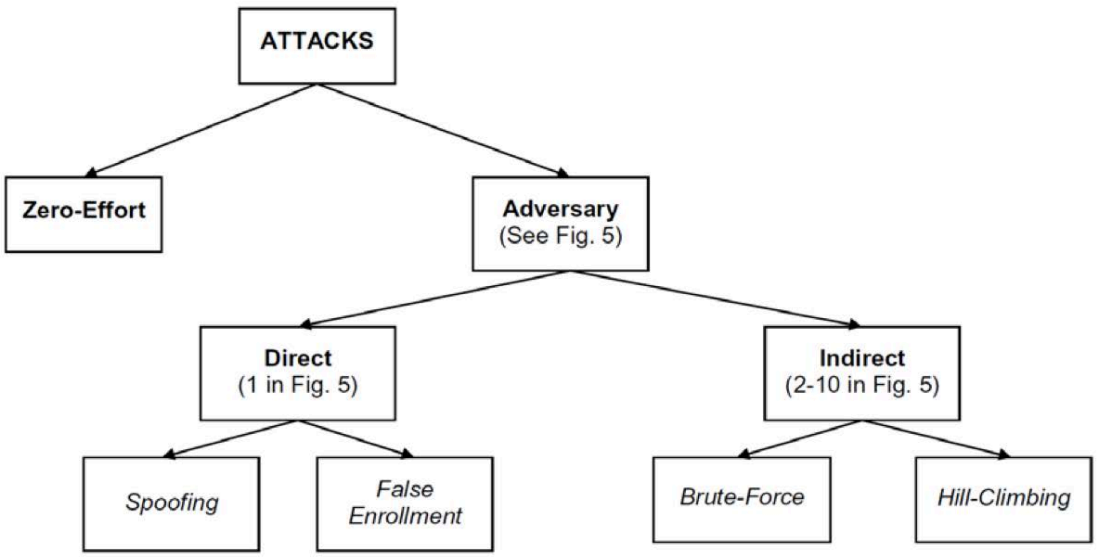


Figura 10. Clasificación de tipos de ataque a sistemas biométricos [9]

En primera instancia el ataque se divide en ataques Zero Effort/Esfuerzo cero o bien en ataques Adversary/Adversario. La principal diferencia es que en los adversarios existe una intención y una acción específica para autentificarse con otra identidad mientras que el esfuerzo cero proporciona una identificación sin necesidad de ninguna acción, tan solo debido a fallos de procesamiento (FAR y FRR). Por lo tanto:

- **Ataques Zero-Effort (Sin esfuerzo):** Son ataques que no requieren de un esfuerzo ni ninguna acción porque el reconocimiento se realiza de forma que sin hacer nada podemos suplantar una identidad. Están basados en la FRR y la FAR.

- **Ataques Adversary (Adversario):** Se basa en que existe un atacante malicioso que quiere vulnerar el sistema. Su clasificación depende de, en que punto y de que forma interviene en el proceso de reconocimiento.

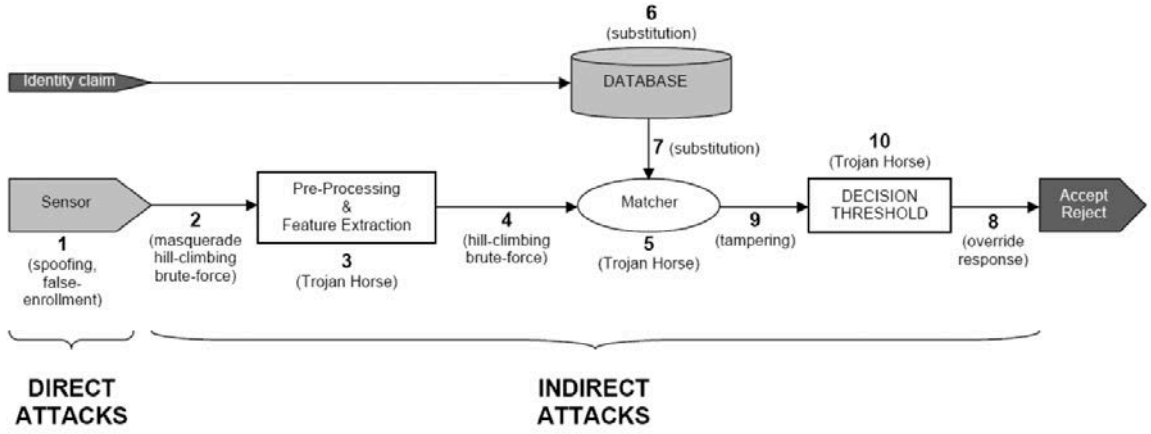


Figura 11. Clasificación de ataques Adversary/Adversario [9]

Como se observa en la figura 10 y 11, los ataques adversario se dividen en directos o indirectos. Los directos se enfocan en la muestra biométrica real propiamente dicha, mientras que los ataques indirectos se centran en el procesamiento interno digital y en comparación de la muestra.

Ataques Direct (Directos): Se basan en modificar la muestra biométrica física que se introduce en el sistema. Como ataques más comunes se encuentran el False Enrollment / Falso reclutamiento que como su propio nombre indica es reclutar una muestra falsa o Spoofing / Engaño suplantando la identidad de otro usuario existente en la base de datos mediante una muestra falsa copiada del usuario a suplantar.

Ataques Indirect (Indirectos): Por un lado en los ataques Brute-Force / fuerza bruta, que se basan en introducir todas las posibles combinaciones hasta conseguir vulnerar el sistema, por ejemplo, probar todas las combinaciones de un Personal Identification Number (PIN). Por otro lado están los Hill-Climbing, que manipulan las características del procesamiento de la muestra biométrica de forma que coincida en las características que se busque [11].

Se debe aclarar que existen más ataques y que estos se están actualizando constantemente. Será parte del trabajo del evaluador investigar para identificar ya no sólo ataques clásicos sino de informarse de los últimos nuevos ataques y catalogar estos ataques si es posible.

Una vez se tiene claro a qué sistema se enfrenta, qué características tiene y qué tipo de ataque se quiere realizar es cuando entra en juego la habilidad del propio evaluador para conseguir información referente a su TOE y a sus ataques. Como se ha dicho durante el documento, cuanta más información se tenga, mejor. Gran parte del trabajo de evaluación se encuentra en este punto y además puede repercutir en el resto de la evaluación de no encontrarse los métodos adecuados para vulnerar un sistema.

La herramienta más útil para realizar esta tarea es internet. Se pueden encontrar desde artículos con información de ataques, vídeos con la realización, tutoriales, etc.

3.3 Fase 2: Estudio y definición de los ataques

En este apartado se buscará una definición concreta de los ataques que se quieren realizar y que en teoría pueden vulnerar el sistema, incluyendo los pasos para su realización, sus materiales, etc. También se buscará un análisis teórico de los ataques basado en el cálculo de su potencial de ataque teórico, que posteriormente en una última fase será necesario para calcular la resistencia del TOE. Es muy importante dedicar un gran grueso del tiempo al estudio y definición de los ataques puesto que serán los que finalmente acotarán la seguridad del sistema. Por ejemplo, si con un potencial intermedio logramos vulnerar el sistema, entonces el TOE será vulnerable frente a potenciales de ataque mayores y tendrá resistencia a ataques con menor potencial.

3.3.1 Definición de ataque

Llegado a esta fase ya se debe haber buscado información referente a los ataques que se quieren hacer. Sin embargo, hace falta definir el ataque completamente para su posterior estudio y ejecución. La recomendación que se adopta en este trabajo es escribirlo a modo de receta bajo el siguiente esquema:

- **Nombre / Referencia**

- **Definición del ataque:** En qué consiste, cómo se va a hacer, qué situaciones particulares hacen falta, y sus características más relevantes.

- **Materiales:** Lista de materiales necesarios para la ejecución del ataque, debe de incluir hasta el más mínimo detalle y referencias a materiales especiales en caso de ser necesario.

- **Pasos:** Listado de los pasos ordenados de forma secuencial para la realización del ataque. Deberá incluir hasta la realización intermedia de materiales para el ataque.

- **Referencias:** Si las hay, incluir referencias a videos, tutoriales o papers para facilitar la realización del proceso de ejecución.

3.3.2 Cálculo de potencial de ataque

El objetivo de un evaluador es calcular la resistencia del TOE a los ataques, es decir, evaluar su seguridad. Como se dijo en el anterior apartado la resistencia del TOE dependerá de los ataques que logren o no vulnerar el sistema, y de que potencial de ataque tenían los ataques ejecutados. Para ello se comenzará definiendo la clasificación de potenciales de ataque y posteriormente, definiendo su cálculo.

Los potenciales de ataques se catalogan desde Básico (AVA_VAN.1 y AVA_VAN.2), Intermedio (AVA_VAN.3), Moderado (AVA_VAN.4) hasta Avanzado (AVA_VAN.5) [5]. Más adelante se verán las características de cada uno de ellos, pero a rasgos generales se puede decir, que a más potencial de ataque mayor será el conocimiento técnico, costará más dinero debido a un equipo mucho más técnico y llevará mucho más tiempo desarrollarlo.

Para calcular dicho potencial se van a tener en cuenta los criterios de evaluación de Common Criteria [5] que cuenta con los siguientes factores:

- Tiempo necesario para identificar y desarrollar el ataque (**Elapsed Time**).
- Requerimientos técnicos específicos (**Specialist Expertise**).
- Conocimiento del TOE (**Knowledge of the TOE**).
- Oportunidades (**Window of opportunity**).
- Equipo necesario (**IT hardware/software or other equipment**).

A continuación se entra en detalle en cada uno de los factores con el propósito de catalogar los distintos niveles que conformarán una puntuación para realizar el cálculo del potencial de ataque:

- **Elapsed time (Tiempo transcurrido)** es el tiempo total necesario para que el atacante o evaluador identifique una posible vulnerabilidad en el TOE, incluyendo el tiempo de desarrollo del ataque y su ejecución. Siempre se considera en este factor el peor escenario posible para estimar la cantidad de tiempo. Se puede dividir en los siguientes intervalos correspondientes a diferentes niveles:

a) Menos de un día.

b) Entre 1 día y 1 semana.

c) Entre 1 semana y 2 semanas.

d) Entre 2 semanas y 1 mes.

e) Más de un mes, y cada mes extra aumenta el nivel hasta los 6 meses.

f) Más de 6 meses.

- **Specialist Expertise (Experiencia especialista)** se refiere al nivel de conocimiento específico de los principios básicos del sistema (protocolos, sensores, etc.), del producto o de métodos de ataque. Dentro de esta categoría se catalogan en niveles:

a) Layman / Ignorante: Ignorante frente a expertos, sin conocimiento específico.

b) Proficient / Hábil: Con conocimientos de seguridad del sistema en lo que les es familiar. Cuando varias personas de nivel proficient son necesarias para realizar el ataque el nivel sigue siendo Proficient.

c) Expert / Experto: Expertos que conocen los principios algorítmicos, protocolos, hardware, estructuras, seguridad, técnicas y herramientas para realizar nuevos ataques y con capacidad de realizar ataques clásicos, muy relacionados con el sistema.

d) Multi-Expert / Multi experto: Experto en diferentes campos de aplicación para los ataques.

- **Knowledge of the TOE (Conocimiento del objetivo)** se refiere a información especializada en relación al TOE. Es distinto al anterior apartado, pero si tienen relación. Los diferentes niveles son:

a) Public / Público: Conocimiento adquirido de información pública del TOE (ejemplo, de internet).

b) Restricted / Restringido: Conocimiento adquirido de información restringida del TOE (ejemplo, información para desarrolladores).

c) Sensitive / Sensible: Conocimiento de información delicada sobre el TOE (ejemplo, información restringida a ciertos miembros del equipos de desarrolladores).

d) Critical / Critico: Conocimiento de información crítica sobre el TOE (ejemplo, información restringida sólo a pocas personas con información sobre niveles básicos del sistema).

- **Window of opportunity (Ventana de oportunidad)** es uno de los factores determinantes y engloba las oportunidades para enfrentarse al sistema medido en tiempo de acceso y en número de intentos que se pueden realizar. En muchas ocasiones este factor es el que impide la realización de un ataque porque no es posible llevarlo a cabo debido a que se necesita mucho tiempo para hacer pruebas o muchos intentos para probarlo. Los diferentes niveles son:

a) Unlimited access / Ilimitado: Acceso ilimitado lo que significa que el atacante no necesita una oportunidad específica porque hay riesgo de que le detecten mientras accede al TOE y por lo tanto puede acceder todas las veces que quiera.

b) Easy / Fácil: Fácil significa que se debe acceder al TOE durante menos de un día y que el ataque necesita menos de diez intentos para realizarse.

c) Moderate / Moderado: Moderado significa que se debe acceder al TOE durante menos de un mes y que el ataque necesita menos de cien intentos para realizarse.

d) Difficult / Difícil: Difícil significa que se debe acceder al TOE durante al menos 1 mes o que el número de intentos para realizar el ataque sea de al menos cien veces.

e) None / Ninguno: Ninguno significa que la oportunidad no es suficiente para realizar el ataque. El tiempo en el que el TOE es accesible es menor al tiempo que se necesita para ejecutar el ataque (ejemplo, una cerradura que se cambia cada semana y se necesitan dos semanas para llevar a cabo el ataque). También puede ser porque el número de intentos es demasiado grande y el atacante no es capaz de llevarlo a cabo (por ejemplo, tener más probabilidades de destruir el TOE antes de llevar a cabo todos los intentos).

- **IT hardware/ software or other equipment (Equipamiento)** se refiere al equipo requerido para identificar o explotar una vulnerabilidad. Dependiendo de ello existen los siguientes niveles:

a) Standard / Estándar: El equipo necesario se puede conseguir fácilmente, tanto para la identificación de vulnerabilidades como para un ataque. El equipo puede llegar a ser parte del propio TOE (ejemplo, un debugger de un sistema operativo) o puede ser obtenido fácilmente (ejemplo, descargas de internet, evaluadores de protocolo, etc.).

b) Specialised / Especializado: El equipo necesario es especializado y por lo tanto no es tan sencillo de obtener pero no es necesario un esfuerzo desproporcionado. Se puede obtener una cantidad moderada de equipos o requiere el desarrollo de aplicaciones para el ataque. Si se necesitan varios equipos para distintos pasos en un ataque, entonces su nivel será considerado como Bespoke / a medida.

c) Bespoke / A medida: Equipamiento a medida que no es fácil conseguir para el público, bien porque necesita ser desarrollado o porque al ser un equipo tan específico que su distribución está controlada o restringida. Además, suele ser un equipamiento muy caro.

d) Multi-Bespoke / Múltiple a medida: Equipamiento a medida para diferentes pasos dentro de un mismo ataque.

Una vez se ha asignado un nivel para cada factor del potencial de ataque se debe acudir ir a la tabla 1 de la siguiente página y asignar el valor correspondiente al nivel seleccionado. Todo ello sumado dará un número correspondiente al potencial del ataque.

Potencial de ataque = Tiempo transcurrido + Experiencia especialista + Conocimiento del objetivo + Ventana de oportunidad + Equipamiento

Para potencial de ataque total entre 0-9 se cataloga como Básico (AVA_VAN.1 y AVA_VAN.2), entre 10-13 es Intermedio (AVA_VAN.3), entre 14-19 es Moderado (AVA_VAN.4), entre 20-24 es Avanzado (AVA_VAN.5) y 25 o más, es Profesional o más que Avanzado según [5].

Este método es una aproximación básica. En muchos casos no tendrá en cuenta todos los factores existentes y sin embargo, afectarán a la resistencia del TOE y al potencial de ataque. Por ejemplo, la presencia de una vulnerabilidad puede hacer que otras vulnerabilidades del sistema sean más fáciles de explotar, cambiando completamente la seguridad del sistema. Este tipo de factores deberán ser indicados y valorados por el propio evaluador ya sea aumentando el potencial de ataque o bien disminuyendo el nivel de resistencia del TOE. En cualquier caso siempre se debe imaginar el peor escenario posible para la valoración.

Factor	Valor
Tiempo transcurrido	
<= un día	0
<= una semana	1
<= dos semanas	2
<= un mes	4
<= dos meses	7
<= tres meses	10
<= cuatro meses	13
<= cinco meses	15
<= seis meses	17
> seis meses	19
Experiencia especialista	
Ignorante	0
Hábil	3
Experto	6
Multi experto	8
Conocimiento del objetivo	
Pública	0
Restringido	3
Sensible	7
Crítico	11
Ventana de oportunidad	
Ilimitado	0
Fácil	1
Moderado	4
Difícil	10
Ninguno	Sistema no explotable
Equipamiento	
Estándar	0
Especializado	4
A medida	7
Multiple a medida	9

Tabla 1. Valores de los factores del potencial de ataque [5]

3.3.3 Viabilidad económica y técnica del ataque

Antes de entrar en profundidad en los pasos a seguir en esta fase de penetración habrá que valorar de las limitaciones que puede llegar a tener un cierto ataque para ser ejecutado en base a factores que hasta ahora no habían sido considerados. Para ello se realizará un estudio de viabilidad económica y técnica.

En el estudio se debe valorar si como evaluador, es posible realizar el ataque, ya que no vale definir ataques y estudiarlos si luego no se pueden poner en práctica. Será aquí cuando se analicen dichos factores.

Existen factores determinantes como puede ser que la ventana de oportunidad sea nula y por lo tanto no se pueda vulnerar el sistema porque no se tiene acceso a él. También podría darse el caso de que el material necesario para ejecutar el ataque no se pueda conseguir ya sea porque sea material muy restringido o porque su coste es demasiado alto.

Se debe analizar si el ataque es rentable desde el punto de vista del atacante o evaluador en este apartado. Además se añadirá el punto de vista del receptor del ataque que hasta ahora no había sido contemplado.

Desde el punto de vista del atacante la inversión de realizar todo este estudio y ejecución debe de ser rentable como principio básico al beneficio que se pretende conseguir vulnerando el sistema. En caso de no ser así, generalmente no se llegará a ejecutar por su índice de rentabilidad negativo.

En el caso del receptor del ataque, una vez se demuestra que el ataque puede vulnerar su sistema tiene dos opciones, mejorar o no el sistema. Es posible que desde un punto de vista económico sea más rentable que sea vulnerable puesto que las pérdidas por un posible ataque son menores que la inversión para actualizar el sistema frente a la amenaza. Esto se analizará en el informe de seguridad.

3.4 Fase 3: Penetración o pruebas

Esta es la última y tercera fase de la metodología para le evaluación de la seguridad. Será donde se probará y demostrará si experimentalmente el/los ataque/s logran vulnerar o no el sistema biométrico.

Lo apropiado es probar todos los ataques posibles para dividirlos posteriormente en ataques que han tenido éxito y cuáles no, de forma que se pueda catalogar la seguridad del sistema y su resistencia que es el fin de toda esta metodología.

Además se darán unas pautas para realizar las pruebas en términos de calidad, aceptación del sensor, captura del sensor y procesamiento.

3.4.1 Pruebas

Anteriormente se definió en la fase de estudio y definición de los ataques, una receta para cada uno de los ataques que se quiere realizar, por lo tanto, es seguir los pasos definidos ahí lo que se debe hacer. El problema llega a la hora de analizar los resultados, donde existen dos visiones, desde el punto de vista de la seguridad y desde el punto de vista biométrico.

Desde el punto de vista de la seguridad, con que un ataque logre vulnerar el sistema una vez, implica que dicho sistema es vulnerable y por lo tanto, no seguro. Por otro lado, el punto de vista de la biometría se centra más en el porcentaje de éxito de dicho ataque (al menos del 50%), por lo tanto no vale solo una vez, sino que de forma generalizada vulnere el sistema.

Será decisión del propio evaluador dependiendo del sistema que quiera vulnerar, el aplicar uno de los dos puntos de vista. Si por ejemplo, de la seguridad del sistema depende algo tremendamente importante como un control de fronteras, sería conveniente utilizar el punto de vista de la seguridad mientras que si estamos evaluando la aceptación de un sensor en particular en laboratorio, interesará más un punto de vista biométrico.

En la mayoría de los casos aplicar la estadística para sacar conclusiones del ataque suele ser inviable económicamente, por ello se usa una población de pruebas mucho más pequeña de lo que la estadística dictamina para que un resultado sea significativo. Por lo tanto, la cantidad de intentos y de muestras necesarias para la realización del ataque quedará también sujeto a la opinión del evaluador.

Sin embargo, se darán unas pautas sobre los procesos de comprobación que se deben realizar para garantizar un mayor éxito del ataque. El proceso de pruebas consiste en cinco fases:

- 1º Fase: Obtener las muestras biométricas falsas: Se necesitarán usuarios que representen a la población que generalmente use el sistema. Los factores que pueden afectar al estudio suelen ser la edad y sexo.
- 2º Fase: Comprobar la calidad de las muestras: Inspección visual es el método más sencillo de comprobar visualmente la calidad de la muestra. Sin embargo dependerá del tipo de rasgo biométrico falsificado los puntos donde fijarse para comprobar dicha calidad. Con esta inspección se pueden descartar las muestras de peor calidad que claramente no van a servir. También puede realizarse una prueba con algoritmos para determinar la calidad de la muestra.
- 3º Fase: Comprobar si el sistema detecta la muestra: Se debe comprobar si el sistema detecta la muestra como el rasgo biométrico que debería ser. Comprobar el Failure to Detect (FTD), tasa que devuelve el porcentaje de fallo del sistema al no reconocimiento de una muestra biométrica.
- 4º fase: Comprobar si el sistema captura la muestra: Se debe comprobar si el sistema es capaz de capturar la muestra introducida, no sólo de detectarla. Comprobar el Failure to Capturet (FTC), tasa que devuelve el porcentaje de fallo del sistema a la no captura de una muestra biométrica.

- 5º Fase: Comprobar el procesamiento digital de la muestra: Es el último paso de la fase de pruebas y directamente va asociada a la captura de la muestra, puesto que si es capaz de capturarla, es capaz de procesarla digitalmente. Realmente esta fase no está sujeta al evaluador pero en teoría si la muestra tiene la calidad apropiada y no existe fallo al detectar ni al capturar, el ataque debería vulnerar el sistema. Los modos de procesamiento digital incluyen su comparación 1-1 en modo verificación y modo identificación 1-N.

Para la realización de las pruebas se empezará por los ataques con potenciales más bajos a los más altos ya que la resistencia del TOE se basará en el ataque satisfactorio con potencial más bajo. Una vez se hayan ejecutado los ataques se deben dividir en dos grupos: Los que han funcionado y los que no han funcionado.

A partir de este punto, será el grupo de ataques que han funcionado los que se tengan en cuenta para calcular la resistencia del TOE en el siguiente apartado.

3.4.2 Calcular la resistencia del TOE

Para determinar la resistencia del TOE a potenciales vulnerabilidades o ataques, se deberán usar aquellos ataques que hayan vulnerado el sistema satisfactoriamente en la fase de pruebas. Puesto que en la fase de estudio y definición de los ataques se ha calculado el potencial de ataque de cada uno de los ataques, se deberá aplicar la tabla 2 para catalogar el sistema [5]. Donde valor es el potencial de ataque calculado en la fase 2.

Valor	Potencial de ataque necesario para explotar el sistema:	Resistencia del TOE a ataques con potencial de nivel:	Seguridad frente a potenciales de nivel:	Fallo frente a potenciales de nivel:
0-9	Básico	Ninguno	-	AVA_AVAN.1 AVA_AVAN.2 AVA_AVAN.3 AVA_AVAN.4 AVA_AVAN.5
10-13	Intermedio	Básico	AVA_AVAN.1 AVA_AVAN.2	AVA_AVAN.3 AVA_AVAN.4 AVA_AVAN.5
14-19	Moderado	Intermedio	AVA_AVAN.1 AVA_AVAN.2 AVA_AVAN.3	AVA_AVAN.4 AVA_AVAN.5
20-24	Avanzado	Moderado	AVA_AVAN.1 AVA_AVAN.2 AVA_AVAN.3 AVA_AVAN.4	AVA_AVAN.5
25 o más	Profesional	Avanzado	AVA_AVAN.1 AVA_AVAN.2 AVA_AVAN.3 AVA_AVAN.4 AVA_AVAN.5	-

Tabla 2. Clasificación de resistencia del TOE [5]

Aplicando la Tabla 2 a los ataques que han logrado vulnerar el sistema se puede acotar la resistencia del TOE. El sistema por lo tanto, tendrá una buena seguridad frente a ataques con potencial menor al que le vulneró y tendrá debilidad frente a ataques con mayor potencial. En general, es recomendable probar ataques con diferentes potenciales para acotar su seguridad de forma más precisa. Es posible que un ataque con potencial intermedio vulnere el sistema, pero que también lo haga un ataque con potencial básico y por lo tanto, la seguridad del sistema sea básica. Siempre se concluirá que la resistencia del TOE es la calculada por el ataque de menor potencial que haya sido satisfactorio.

3.5 Informe de seguridad

El estudio de la seguridad del sistema biométrico se da por finalizado porque se sabe cuál es el nivel de seguridad del sistema bajo evaluación y que tipo de ataques son propensos a vulnerarlo.

Este apartado es un informe general de la seguridad del sistema, cómo se ha llegado a vulnerar, sus puntos débiles, sus puntos fuertes, qué mejoras en el sistema podrían incrementar la seguridad, la viabilidad de esas mejoras, etc.

4 Metodología de evaluación de la seguridad para sistemas ABC

4.1 Introducción

Anteriormente se definió una metodología de evaluación de la seguridad para cualquier sistema biométrico, sin embargo, esta sección se centrará en los sistemas ABC, en concreto los españoles. Con este documento se pretende analizar de principio a fin una evaluación de seguridad de un sistema ABC, desde el desarrollo de la idea hasta la ejecución de las pruebas y el análisis de los resultados.

El estudio tendrá 3 fases: Identificación del objetivo, estudio y definición de los ataques y por último, fase de penetración o pruebas.

Después, tras concluir la fase de pruebas y calcular la seguridad del sistema se incluye un apartado para redactar un informe acerca de todo el proceso realizado y su posible mejora de la seguridad.

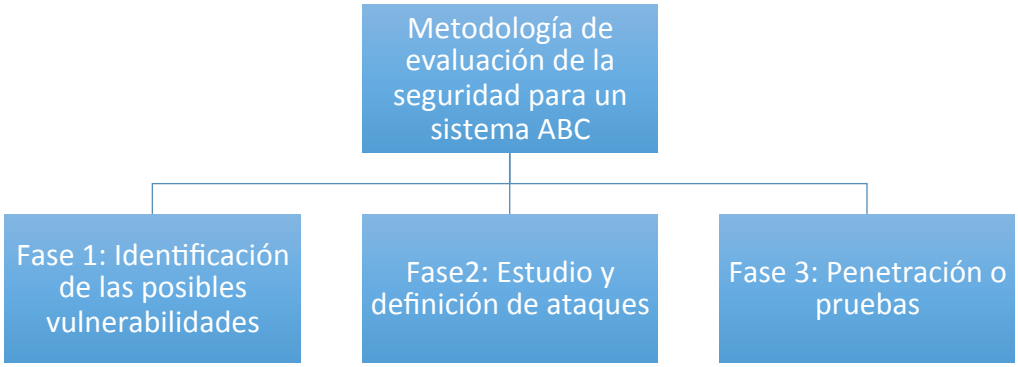


Figura 12. Fases de la metodología de evaluación de la seguridad

4.2 Fase 1: Identificación de posibles vulnerabilidades

A pesar de focalizar el estudio sobre un sistema ABC concreto, el concepto de desarrollo es el mismo y por lo tanto, será necesario encontrar toda la información posible referente a este sistema. Una buena forma de conseguir información técnica es averiguar quién fue el contratista principal del proyecto. Generalmente suele haber un pliego o información pública sobre los contratos entre el ministerio correspondiente y el contratista. Para seguir con el ejemplo de los aeropuertos españoles, se puede ver en [12] que fue Indra el encargado de montar estos sistemas.

Con este punto de partida se debe encontrar cualquier tipo de información relevante para su evaluación. Esto incluye su localización, sus condiciones ambientales, que reconocimiento usa, que sensores utiliza, que algoritmos y muchas cosas más que se verán en los siguientes apartados.

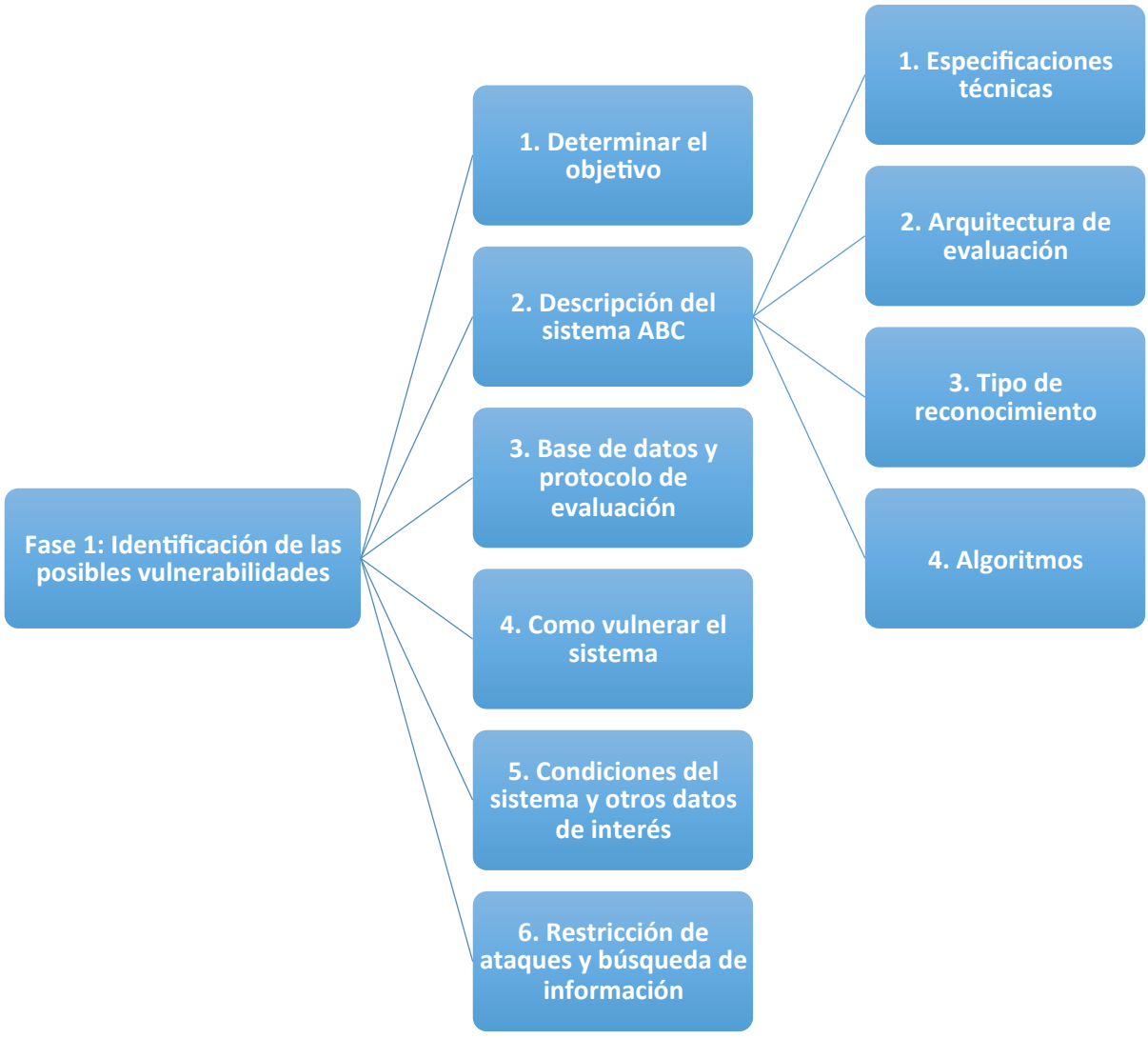


Figura 13. Esquema detallado de la fase de identificación de posibles vulnerabilidades

4.2.1 Determinar el TOE

Se quiere evaluar la seguridad de un sistema automático de control de fronteras (sistema ABC). En concreto se ejemplificará la metodología con los sistemas ABC españoles.

4.2.2 Descripción del sistema

En este apartado se debe conseguir toda la información posible referente a sus especificaciones técnicas o su evaluación (sensores, algoritmos, servicios, etc.) para identificar posibles vulnerabilidades y así centralizar la búsqueda de información. En este proceso se incluirá la arquitectura de evaluación y las especificaciones técnicas físicas de cada sistema ABC. Es la parte más técnica y más detallada de la evaluación. Se basará en las características específicas de los sistemas ABC españoles [13] como ejemplo para la evaluación de la seguridad.

4.2.2.1 Especificaciones técnicas del sistema

Existen dos tipos de sistemas ABC en los aeropuertos, los PCD (Puesto de Control Desatendido) y los PDA (Puesto de Control Atendido). La diferencia entre ellas, como su propio nombre indica, es la característica de estar o no atendido por una persona responsable. En general, puesto que se pretende automatizar el proceso para el control de fronteras habrá un mayor número de PCDs que de PCAs. Puesto que se intentará suplantar una identidad, sólo interesan los PCDs porque se tendrá más libertad a la hora de realizar un ataque.

Ahora se analizarán las especificaciones de cada sistema: PCD, PCA y servidores centrales. Además se detallará el modelo exacto utilizado en los aeropuertos españoles para posteriormente encontrar limitaciones en su evaluación a modo de ejemplo.

- Especificaciones de un PCD [13]:

- **1 Quiosco de acero o bastidor**: Para restringir el movimiento durante la identificación.
- **1 Personal Computer (PC) industrial**: Para procesar los algoritmos y la información necesaria (Advantech ACP-4320).
- **1 Pantalla táctil / Monitor táctil**: Medio de comunicación con el sistema (ELO TOUCH).
- **1 Altavoz:** Para que la persona sea guiada mediante voz (KENWOOD - KFC - 1329C).
- **1 Lector de pasaportes:** Para la verificación documental (confirmar si el pasaporte es original) y la comprobación de la identidad (3M AT9000 Full Page Reader).
- **1 Lector de tarjetas SmartCard de contacto**: Para la verificación documental e (identificar el DNI o tarjeta de identificación correspondiente y su originalidad), así como para obtener la huella y la foto de la persona a identificar (SCM Microsystem SCR333).
- **1 Lector de huellas dactilares**: Para verificación dactilar Match-On-Card (L SCAN 100 de Crossmatch).
- **3 Cámaras**: Para el reconocimiento facial (Logitech QuickCam Sphere AF).
- **1 Sistema de alimentación ininterrumpida (SAI/UPS):** Para mantener el sistema operativo pese a cualquier problema con el suministro eléctrico.
- **Elementos de iluminación:** Es muy importante para temas de reconocimiento facial tener una iluminación óptima.

Existen 2 tipos de instalación como se puede ver en la Figura 14 y en la Figura 15:

Figura 14. Instalación tipo esclusa

Figura 15. Instalación tipo puerta simple

En el caso de puertas simples la huella se captura con el objeto de permitir el paso al ciudadano en los módulos de acceso (Figura 16).

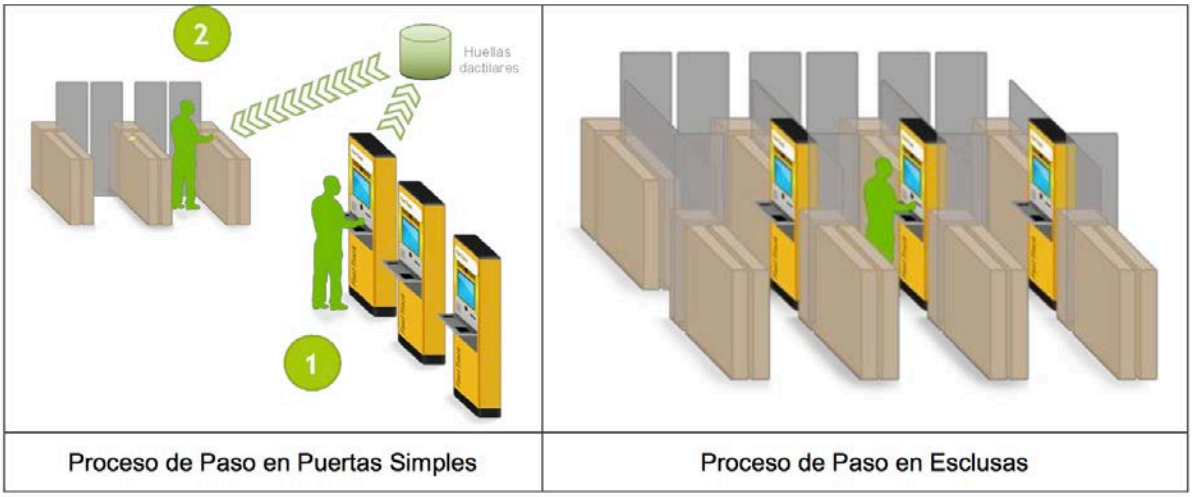


Figura 16. Diferentes módulos de acceso para el control fronterizo [13]

La comunicación entre los PCDs y los servidores de la instalación ABC se realiza mediante servicios Web, de forma que la creación de procesos de paso y su posterior gestión según su resultado, se realiza mediante llamadas entre el PCD y el servidor. Asimismo, el servidor gestiona buzones de comandos y alertas para cada uno de los PCDs, a través de los que los PCDs pueden recoger comandos enviados por el servidor (propios o generados por el Policía desde el PCA), así como enviar alertas referentes al estado de sus dispositivos (averías en cámaras, lectores de huellas, lectores de documentos, fallos en la conexión a sistemas remotos desde el PCD, etc.).

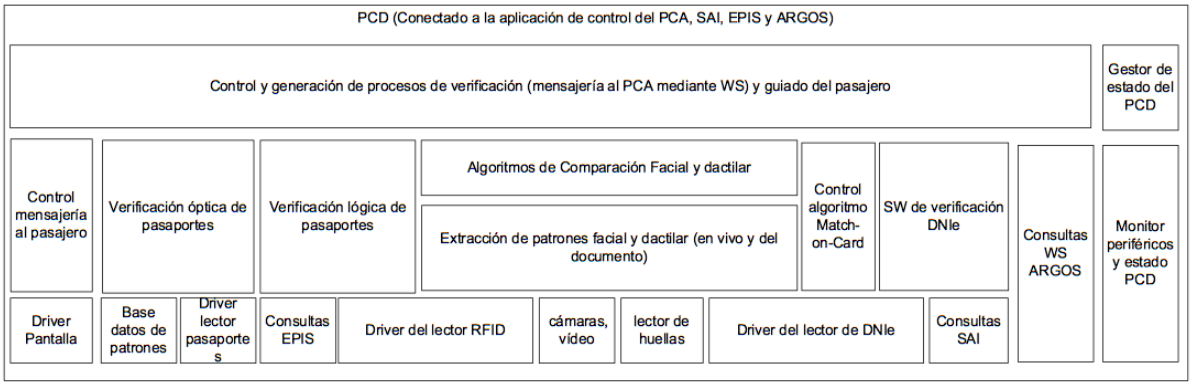


Figura 17. Arquitectura y servicios de la aplicación del PCD [13]

- Especificaciones de un PCA [13]:

- **2 PCs**: Para procesar los algoritmos y la información necesaria (HP8000E).
- **3 Monitores:** Medio de comunicación con el sistema (2 x HPL1951g y 1 x ELO TOUCH).
- **1 Lector de pasaportes:** Para verificación documental e identificar si el pasaporte es original y confirmar la identidad (3M AT9000 Full Page Reader).
- **1 Lector de tarjetas SmartCard contacto**: Para verificación documental e identificar el DNI o tarjeta de identificación correspondiente así como para obtener la huella y la foto de la persona a identificar (SCM Microsystem SCR333).
- **1 Lector de huellas dactilares**: Para verificación dactilar (L SCAN 100 de Crossmatch).

En cada frontera existe al menos un PCA instalado en una cabina que monitoriza el paso de los ciudadanos efectuado desde un cierto conjunto de puertas simples o paso en esclusas (Figura 14 y 15). El PCA ofrece tres funcionalidades a los Policías encargados del control fronterizo:

- Monitorización de los procesos de paso en curso y recientes: Permite al Policía encargado del control del PCA conocer los diferentes procesos de verificación que se están produciendo en el sistema. Dicha herramienta, cuya interfaz es operable a través de una pantalla táctil, muestra un resumen de los aspectos fundamentales de cada proceso de verificación (fotografía, tipo de documento, resumen de las verificaciones efectuadas, etc.), permitiendo además obtener mayor grado de detalle de cada uno de estos procesos.

Figura 18. PCA monitorización y supervisión

- Comprobación de nivel 2: Se realiza con una herramienta realizada al efecto integrada con el monitor de pasos y que permite extraer información de éste para efectuar verificaciones adicionales a aquellos pasajeros que no hayan superado con éxito todas las verificaciones. Esta herramienta, integrada con las herramientas de consulta de señalamientos del Cuerpo Nacional de Policía (CNP), se complementa con un lector de pasaportes, un lector de DNI e y un lector de huella dactilar.

Figura 19. PCA biometría y señalamientos

Figura 20. PCA verificación física del documento.

- Monitorización vídeo-vigilancia: Recibe de manera continua las imágenes captadas por las cámaras de cada PCD, de forma que el funcionario de Policía encargado del control del PCA puede observar el comportamiento de los ciudadanos durante su interacción con el sistema.

Por otra parte, el software de monitorización y el de nivel 2 del PCA se conectan al servidor central con los siguientes objetivos:

- Activar y desactivar la instalación completa al iniciar o terminar una sesión de trabajo.
- Recabar información de los procesos en curso en la instalación, tanto para la monitorización del sistema de pasos, como para efectuar verificaciones detalladas en la aplicación de nivel 2.
- Actuar sobre aquellos procesos que requieran atención del usuario, por ejemplo para validarlos, descartarlos, etc.
- Controlar el estado de cada uno de los PCDs, recibiendo las alertas enviadas por estos y enviando los comandos de habilitación/deshabilitación marcados por el usuario.
- Controlar el estado de cada uno de los módulos de acceso, recibiendo los mensajes de estado recabados, así como permitiendo el envío de comandos de apertura, cerrado, bloqueo y desbloqueo correspondientes.

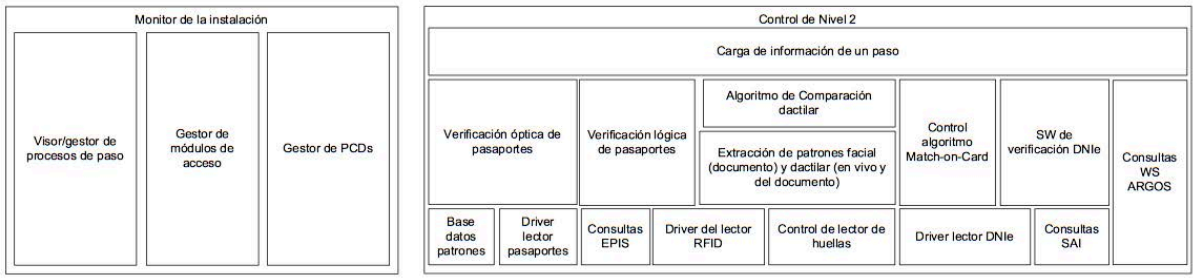


Figura 21. Arquitectura y servicios de las aplicaciones del PCA [13]

El hecho de que haya una PCA restringe la capacidad de movimiento y actuación del evaluador/falsificador ya que de comportarse de forma sospechosa se podrían realizar comprobaciones adicionales e identificar que es una farsa. La forma de evitarlo sería intentar ir a ciertas horas o días cuando haya una mayor afluencia de gente y el responsable del PCA no pueda mantener la atención sobre todos los pasajeros que intentan pasar por la frontera.

- Las especificaciones de los sistemas informáticos están incluidos en un rack con los servidores y elementos de red, que contiene los elementos centrales de la instalación [13]:

- **2 servidores:** Corren el software de control de la instalación y el resto de servicios comunes (lógica de negocio, bases de datos, control de módulos de acceso, etc.) (Fujitsu RX 200 Primergy TX-150 S4).
- **2 switches:** Cisco 2960g.
- **2 cortafuegos con capacidad de balanceo de carga:** StoneGate FW-1030e.
- **Sistema de alimentación ininterrumpida (SAI-UPS):** Para mantener el sistema operativo pese a cualquier problema con el suministro eléctrico (APC 5KVA).

Los servicios se encuentran desplegados sobre máquinas virtuales, mediante la infraestructura e hipervisor XenServer de Citrix. De este modo, sobre cada servidor existe una máquina virtual como servidor de aplicaciones JAVA, que ejecuta la lógica del sistema sobre un servidor GlassFish, así como un servidor de base de datos, basado en MySQL. Los servidores están configurados en redundancia Activo-Pasivo.

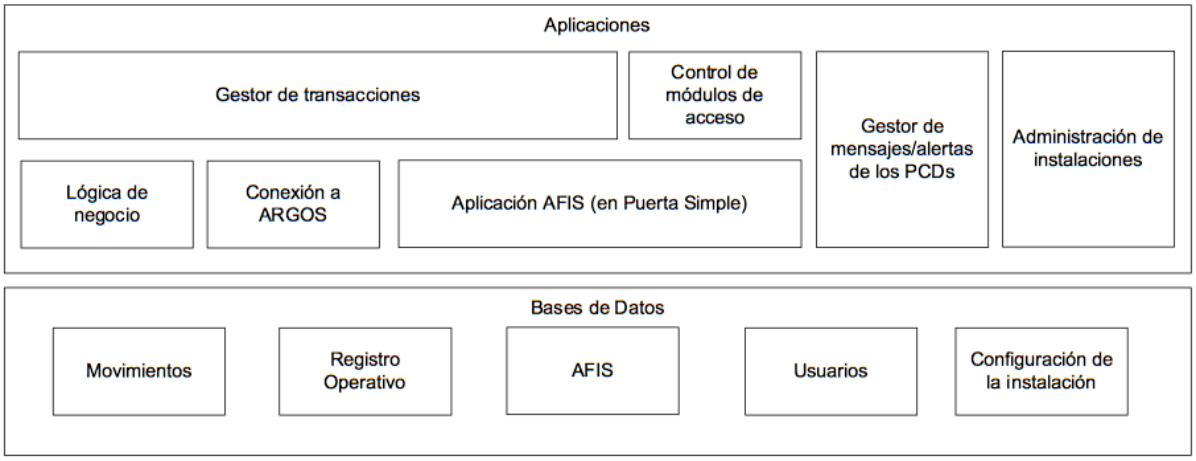


Figura 22. Arquitectura y servicios del servidor local [13]

Se supone que los servidores centrales y sistemas informáticos tienen una buena seguridad por lo que prácticamente se descarta cualquier ataque informático. Por otro lado, la verificación documental se encuentra fuera del estudio biométrico.

En la descripción del sistema se puede ver que los únicos reconocimientos a tener en cuenta es el facial con cámara Logitech QuickCam Sphere AF y el dactilar, con el sensor L SCAN 100 de Crossmatch. Cuando haya que detallar los diferentes ataques a sensores de huella y al reconocimiento facial, se hará referencia a estas especificaciones.

4.2.2.2 Arquitectura de evaluación

Guía sobre los pasos que sigue el sistema para la verificación de la identidad del individuo y por lo tanto, los pasos que deben seguir los evaluadores en los ataques para ir vulnerando cada una de las fases del reconocimiento. Dentro de la arquitectura de evaluación existen diferentes arquitecturas o modelos de uso dependiendo de si es un pasajero, un falsificador/evaluador o el control fronterizo.

El pasajero sigue el software de guiado y las instrucciones que se presentan en una pantalla táctil para efectuar el proceso; El falsificador/evaluador aparte de seguir el software de guiado tendrá que seguir las pautas de sus ataques; El control fronterizo seguirá el proceso del pasajero y además, verificará que el proceso sea realizado debidamente.

Descripción del modelo de uso y proceso de verificación de un pasajero:

1) Inserción del documento electrónico de viaje, ya sea el pasaporte electrónico o el DNI e. En él se encontrará toda la información para comparar las características biométricas que se van a introducir.
2) Verificación facial tomando fotos en vivo con las cámaras y comparando con la foto extraída del documento de identificación.
3) Verificación biométrica dactilar en caso de que el documento insertado disponga de este marcador biométrico, el pasajero es guiado al correspondiente lector de huellas. En caso de que sea una Puerta Simple, la huella se captura con objeto de permitir el paso al ciudadano en los módulos de acceso (Figura 15 y 16).
4) En este punto el pasajero es indicado sobre cómo y por dónde debe proceder para finalizar su cruce fronterizo. Dichas instrucciones dependerán de las verificaciones efectuadas de forma que o puede cruzar la frontera por los módulos de acceso automáticos y bien por un PCA donde el funcionario correspondiente efectuará comprobaciones adicionales.

Descripción del modelo de uso y proceso de verificación de un falsificador/evaluador:

1) Inserción del documento electrónico de viaje, ya sea el pasaporte electrónico o el DNI e. En él se encontrará toda la información para comparar las características biométricas que se van a falsificar.
2) Ejecución del ataque para la verificación facial.
3) Ejecución del ataque para la verificación biométrica dactilar. En caso de que sea una Puerta Simple, la huella se captura por lo tanto al salir por dicha puerta deberá ejecutar el ataque de verificación dactilar de nuevo (Figura 15 y 16).
4) En este punto el falsificador/evaluador es indicado sobre cómo y por dónde debe proceder para finalizar su cruce fronterizo. En caso de ser guiado a un PCA la realización de los ataques se complica puesto que habrá una vigilancia humana que reaccionará frente a conductas inusuales.

Descripción del modelo de uso y proceso de verificación desde el punto de vista del control fronterizo:

1) Verificación documental:

- Verificación óptica: Se efectúa sólo en el caso de los pasaportes. El lector de pasaportes captura imágenes en luz visible, ultravioleta (UV) e infrarroja (IR) y compara el documento con una base de datos de patrones ubicada en cada equipo localmente con el fin de identificar la autenticidad del documento.

- Verificación lógica: Se efectúa para todos los documentos.
  - En el caso de los pasaportes, la verificación lógica cubre todas las comprobaciones obligatorias y opcionales del estándar International Civil Aviation Organization ICAO 9303, así como las verificaciones adicionales disponibles en pasaportes electrónicos de 2ª generación. Para la validación de la firma electrónica de los pasaportes, el sistema se conecta al sistema de Inspección de Pasaportes (EPIS) del Cuerpo Nacional de Policía (CNP), si bien en caso de que esta conexión no sea posible, la verificación se puede ejecutar en el propio PCD, haciendo uso de los certificados guardados en su caché.

  - En el caso del DNI e, la verificación lógica se efectúa mediante la conexión con los sistemas del CNP, que permite la validación del documento y el acceso a sus zonas de datos protegidas.

2) Verificación biométrica facial:

El sistema extrae la imagen patrón almacenada en el documento y la compara con las fotografías tomadas en vivo al pasajero. Adicionalmente, en el caso de los pasaportes, se compara la imagen patrón electrónica con la capturada de la página biográfica del documento.

3) Verificación biométrica dactilar:

En aquellos documentos en los que dicho marcador biométrico está disponible y es accesible, el sistema captura una huella dactilar del pasajero y la compara con el patrón almacenado en el documento. En el caso del pasaporte de 2ª generación esta comparación se ejecuta con la ayuda de un algoritmo de biometría externo, mientras que para el DNI e se apoya en su algoritmo Match-On-Card (MoC). Nótese que en las instalaciones de Puerta Simple la captura de huella dactilar se efectúa en todo caso, dado que ésta se utiliza posteriormente para habilitar el cruce de la frontera por los módulos automáticos de acceso.

4) Verificación en las bases de datos de señalamientos del CNP:

Siguiendo la legislación vigente en el control de fronteras de ciudadanos Schengen, se efectúan las siguientes comprobaciones:

- Comprobación de los datos personales del pasajero contra la base de datos de señalamientos de la Policía de acuerdo con el Código de Fronteras Schengen.

- Comprobación del documento en las bases de datos de documentos robados y perdidos.

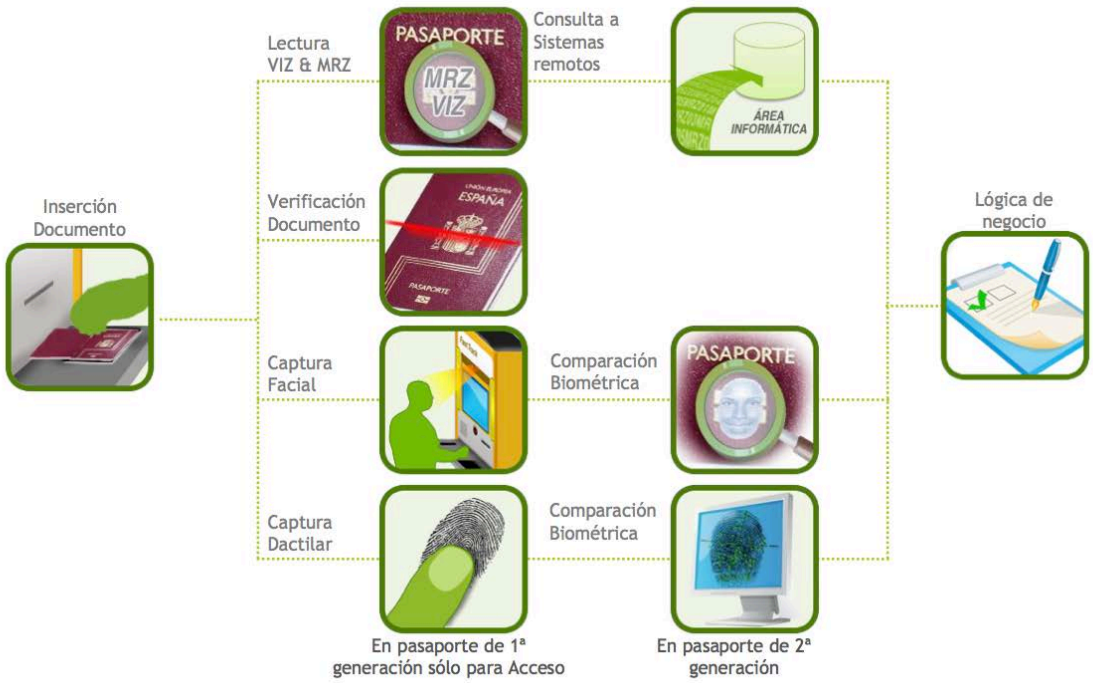


Figura 23. Flujo de verificación de un pasajero portador de un pasaporte electrónico [13]

Tras explicar la arquitectura de evaluación se deberá vulnerar la identificación documental, la verificación dactilar y facial, además ya se sabe la referencia de los sensores que utilizan para la evaluación, los cuales se analizarán en el siguiente apartado. La evaluación documental esta fuera del estudio de la biometría así que se supondrá que se puede conseguir el documento original para la evaluación. Como se vio anteriormente debido al cotejo con diferentes bases de datos del CNP, el documento no puede estar denunciado como robado o perdido puesto que saltarían las alarmas.

4.2.2.3 Reconocimiento dactilar y facial

Como se vio anteriormente existen dos tipos de reconocimiento biométrico en el sistema que se deben vulnerar: El reconocimiento facial y dactilar.

- **Reconocimiento dactilar**

Se buscarán una serie de especificaciones técnicas para analizar el sensor y su seguridad frente a ataques. Para ello se deberán tener en cuenta los siguientes factores:

1. Determinar el tipo de sensor:

Lo primero que se debe hacer es catalogar el tipo de sensor de huella del sistema ABC, ya que esto puede afectar al éxito de los ataques. Cuando se busque información en papers o páginas web, se verá que no todos los ataques valen para todos los sensores. Toda tecnología tiene sus limitaciones, con sus pros y sus contras. Se aprovecharán esas características para focalizar hacia cierto tipo de ataque posteriormente.

Existen los siguientes tipos de sensores [14]:

- Ópticos reflexivos

Consiste en colocar el dedo sobre una superficie de cristal que está iluminada por un diodo LED. Cuando las crestas de la huella tocan la superficie, la luz es absorbida, mientras que entre dichas crestas se produce una reflexión total. La luz resultante y las zonas de oscuridad son registradas.

Existen factores que empeoran el funcionamiento del sensor: Las imágenes obtenidas con dedos húmedos y secos son muy diferentes; Es fácil de engañar y si la piel está deteriorada o dañada, la huella no se reconoce correctamente; El reconocimiento de personas mayores es difícil por insuficiencia de elasticidad lo que puede producir un reconocimiento falso; Si la huella almacenada fue tomada con menos presión, se pueden producir aceptaciones falsas (FAR alta).

- Ópticos transmisivos

Funcionan sin contacto directo entre el dedo y la superficie del sensor. La luz pasa a través del dedo mientras que una cámara toma una imagen directa de la huella dactilar.

La humedad no produce ninguna dificultad. El sensor ve a través de la superficie de la piel sobre una superficie más profunda y produce una imagen multiespectral. El uso de diferentes longitudes de onda para generar imágenes proporciona información de diferentes estructuras subcutáneas, indicación de que el objeto en cuestión es un dedo genuino. Sólo unos dedos artificiales muy precisos podrían vulnerar este sensor.

- Capacitivos

El sensor es un circuito integrado de silicio cuya superficie está cubierta por un gran número de elementos transductores. Cada elemento contiene dos electrodos metálicos adyacentes. La capacidad entre los electrodos se reduce más cuando detecta crestas y menos cuando detecta el espacio entre ellas.

Como contra se tiene que el sensor es susceptible a las descargas electrostáticas. Que además sólo funcionan con pieles sanas normales (sin durezas, callos, etc.) y que la humedad, la grasa o el polvo pueden afectar a su funcionamiento.

- Mecánicos

Se trata de diminutos transductores de presión que se montan sobre una superficie. Esto sólo proporciona un bit de información por píxel, en lugar de trabajar con una escala de grises u 8 bits. No se usan mucho debido a su baja precisión.

- Térmicos

En este caso se detecta el calor conducido por el dedo, el cual es mayor cuando hay una cresta que cuando hay un valle. La imagen está en la escala de grises que tiene la calidad adecuada incluso con el dedo desgastado, con suciedad, con grasa o con humedad.

- Salida dinámica

En lugar de colocar el dedo de forma estática sobre el sensor, el dedo se desplaza lentamente a lo largo del mismo. Este dispone de una estrecha zona sensible, y genera una secuencia completa de imágenes, las cuales son re-ensambladas, en una imagen completa. Las prestaciones se mejoran de modo apreciable y se garantiza la eliminación de cualquier grasa residual.

La especificación sobre la tecnología utilizada viene en la hoja de características del sensor. Para seguir el ejemplo de los aeropuertos españoles, como ya se vio anteriormente el sensor de los sistemas ABC es el L SCAN 100 de Crossmatch que corresponde con un sensor óptico reflexivo.

Otras especificaciones de interés del sensor [15]:

2. Resolución del escáner: Es la resolución máxima que puede alcanzar la muestra. En el caso del L SCAN 100 de Crossmatch es de 500 ppi (Pixeles per inch).

3. Rango dinámico del escáner: Define la calidad de la imagen dependiendo de los bits. En el caso el L SCAN 100 de Crossmatch está en escala de grises lo que significa en 8 bits.

4. Calidad de la imagen: En muchos casos se asocia la calidad de la imagen a la aprobación del estándar del FBI llamado Image Quality Specification (IQS) del FBI's Electronic Fingerprint Transmission Specification (EFTS). El L SCAN 100 de Crossmatch tiene esta calidad de imagen.

5. Resolución de la imagen de salida: Se suele medir en pixeles. El sensor L SCAN 100 de Crossmatch tiene una resolución de 600x600 píxeles.

6. Condiciones de funcionamiento: Habla de las condiciones ambientales para su correcto funcionamiento expresado en niveles de temperatura, humedad relativa, condensación y luz. En el caso el L SCAN 100 de Crossmatch funciona entre 10º-40º C, con humedad relativa entre 10-80%, sin condensación ni exposición directa de luz.

7. Mantenimiento: En general, el mantenimiento será la limpieza de la superficie. En este caso al ser un sensor óptico reflexivo se aconseja una limpieza antes de su uso para garantizar una superficie limpia y su correcto funcionamiento.

- **Reconocimiento facial**

Lo primero que se debe hacer es catalogar el tipo de reconocimiento facial que usa el sistema ABC, ya que esto puede afectar al éxito de los ataques. Cuando se busque información en artículos o páginas web, se verá que no todos los ataques valen para todos los tipos de reconocimiento. Toda tecnología tiene sus limitaciones, con sus pros y sus contras. Se aprovecharán esas características para focalizar hacia cierto tipo de ataque posteriormente.

1. Tipo de reconocimiento facial [16]:

- Holísticos

Reconocen toda la imagen facial. La forma más simple es el llamado template matching, el problema de éste reconocimiento es que tiene que comparar muchas características (Cada pixel es una característica) y por lo tanto hace que el procesamiento de la imagen y su comparación no sea a tiempo real y por lo tanto ineficiente para muchas aplicaciones como por ejemplo, un sistema ABC.

En base a esta técnica existen otras que correlacionan características entre sí para conseguir reducir la identificación a un menor número de coeficientes y por lo tanto se puedan descartar muchas muestras de forma rápida, aumentando así la velocidad de procesamiento. Las tres principales son:

- Análisis de Componentes Principales (Principal Component Analysis): Funciona proyectando las imágenes faciales sobre un espacio de facciones que engloba las variaciones significativas entre las imágenes faciales conocidas. De esta forma caracteriza la imagen facial de un individuo como la suma de los diferentes pesos de todas las facciones de modo que para reconocer una imagen facial sólo hará falta comparar estos pesos.

- Análisis Lineal Discriminante (Linear Discriminant Analysis): Esta técnica permite utilizar las imágenes de la misma persona para desarrollar un conjunto de vectores característicos donde las variaciones entre las diferentes caras se enfatizan mientras que los cambios debidos a la iluminación, expresión facial y orientación de la cara no.

- Discriminante Lineal de Fisher (Fisher Linear Discriminant): Esta técnica es equivalente al Análisis Lineal Discriminante. Los resultados obtenidos son en general mejores que con otras técnicas, sobre todo cuando varían las condiciones de iluminación o las expresiones faciales porque el método da más peso a zonas como los ojos, la nariz o las mejillas que a la boca, porque son zonas más invariables.

- Locales o geométricos

A partir de la imagen de la cara, se determinan unos puntos geométricos que representen únicamente a esa persona mediante distancias entre esos puntos. Da más prioridad a la falta de errores que al nivel de detalle. Este método de reconocimiento facial es de los más utilizados debido a su simplicidad y velocidad de procesamiento a pesar de no ser el más fiable.

- Técnicas 3D

Utiliza sensores en tres dimensiones (3D) para captar información sobre la forma de la cara. Posteriormente de identifican los rasgos característicos de la cara (la barbilla, el contorno de los ojos, la nariz o los pómulos, etc.), así como información espacial, la textura y la profundidad. Una de las ventajas del reconocimiento facial en 3D es que no les afectan los cambios de iluminación, como pasa en el caso de otras técnicas. Además, otro punto a favor es que pueden reconocer una cara en diferentes ángulos, incluso de perfil. El problema es que es difícil obtener imágenes 3D porque los sensores 3D deben estar muy bien calibrados y sincronizados para adquirir una imagen correctamente.

- Análisis de la textura de la piel

Técnica que usa los detalles visuales de la piel analizando líneas únicas, patrones y detalles evidentes como manchas y/o cicatrices del rostro del sujeto. Al utilizar este tipo de reconocimiento se ahorra tener que recorrer toda la base de datos ya que se pueden descartar imágenes fácilmente.

- Reconocimiento basado en video

Es una técnica que ofrece muchas ventajas frente a otros métodos siempre y cuando se esté en un entorno relativamente controlado y donde el tamaño de la cara sea aceptable. Entre sus ventajas se encuentran que un video proporciona más información debido a que se procesan entre 10-25 imágenes por segundo y puede hacer un seguimiento de los cambios de pose o expresiones faciales.

Para seguir el ejemplo de los aeropuertos españoles, como ya se vio anteriormente el reconocimiento se realiza con una cámara Logitech QuickCam Sphere AF y mediante un reconocimiento geométrico basado en video.

Otras características de interés [17]:

Debido a que la tecnología de reconocimiento 3D aún no está muy desarrollada e implantada en este tipo de sistemas se puede decir que el reconocimiento será en 2D por lo que las cámaras necesitarán unos requisitos mínimos para asegurar la calidad de las imágenes.

2. Resolución de imagen: Como mínimo para asegurar un buen funcionamiento la cámara debe tener una resolución mínima de imagen de 640 x 480 pixeles. La cámara Logitech QuickCam Sphere AF tiene una resolución máxima de 1600x1200 pixeles.

3. Color: En general con tener 8 bits y dar imagen en escala de grises es suficiente, sin embargo, actualmente prácticamente todas las cámaras tienen 24 bits true color. La cámara Logitech QuickCam Sphere AF tiene 24 bits true color.

4. Ratio de muestreo: Si se va realizar reconocimiento basado en video, entonces deberá tener una velocidad de captura de imágenes entre 10-25 FPS (Frames Per Second / Imágenes por segundo). La cámara Logitech QuickCam Sphere AF tiene hasta 20 FPS.

Una vez se han analizado las características del sensor de huella y de la cámara se podrá restringir la búsqueda de información hacia sensores ópticos reflexivos y hacía reconocimiento facial local o geométrico. Además, aparte del propio sistema físico de reconocimiento existen algoritmos específicos para procesar cada tarea, de ello se hablará en el siguiente apartado.

4.2.2.4 Algoritmos de evaluación

Un algoritmo es un conjunto ordenado y finito de operaciones que permite hallar la solución de un problema y será mediante algoritmos, como finalmente se procesen las muestras biométricas introducidas en el sistema.

Es muy importante encontrar información del algoritmo de evaluación pues es posible encontrar limitaciones o información útil. Indra seleccionó VeriFinger como algoritmo de reconocimiento dactilar, VeriLook como algoritmo de reconocimiento facial y MegaMatcher de Neurotechnology como algoritmo de identificación multi biométrico en los sistemas ABC [18]. Se analizarán estos algoritmos como ejemplos para otros que puedan ser usados en otros sistemas ABC.

- **Reconocimiento dactilar**

Factores a tener en cuenta: Tipo de reconocimiento 1-1 o 1-N (uno a muchos); Tolerancia a la traslación, rotación o deformación de la muestra; Tamaño de base de datos capaz de gestionar; Premios/reconocimientos como algoritmo; Gestión de calidad de las muestras; que características o imperfecciones elimina de la muestra; FRR y FAR en pruebas reales.

VeriFinger [19]: Admite tanto reconocimiento 1-1 como 1-N; tiene tolerancia a la traslación, rotación y deformación de la muestra; puede gestionar una base de datos ilimitada; mejor algoritmo de huella conocido; capaz de separar las muestras por calidad y usar las de mejores características; elimina ruido y polvo de las muestras.

Para juzgar la FRR y FAR, Neurotechnology analiza la respuesta del algoritmo frente a diferentes sensores, se elegirá un sensor con características similares al del sistema real (500 pixels-per-inch (ppi), sensor óptico reflexivo, rango de humedad y temperatura parecidos (Temperatura 0ºC-40ºC y humedad 10-90%) y resolución imagen similar (600x600 pixeles)). De las pruebas realizadas el sensor más parecido al L SCAN 100 de Crossmatch es el Verifier 300 LC de Crossmatch.

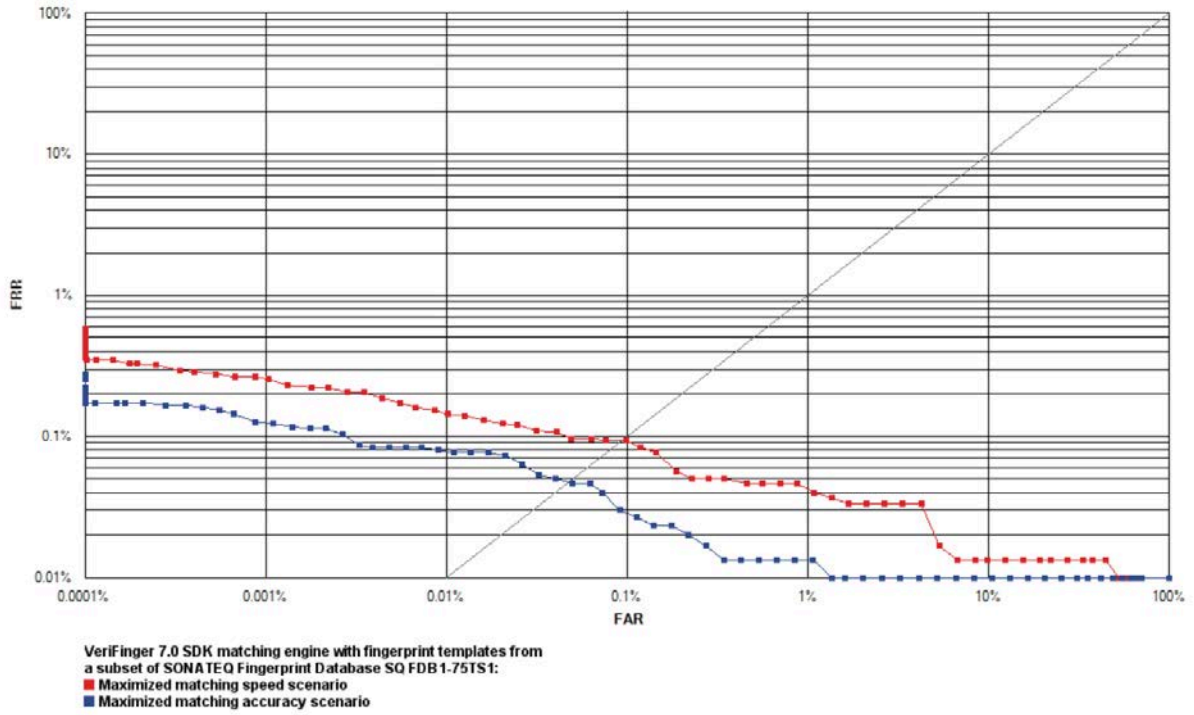


Figura 24. ROC del algoritmo VeriFinger [19]

Como se observa en el gráfico, hace dos análisis del FRR y FAR. La línea roja es con el sistema a la velocidad máxima de procesamiento y la azul, con la mayor precisión posible. Receiver operation characteristic (ROC) se usa para demostrar la calidad de un algoritmo enfrentando FAR / FRR.

El porcentaje de FAR es muy bajo. Este dato se usará después para descartar el tipo de ataque Zero-Effort o esfuerzo cero.

- **Reconocimiento facial**

Factores a tener en cuenta: Tipo de reconocimiento 1-1 o 1-N (uno a muchos); Capacidad de reconocer caras vivas y no fotografías; Capaz de reconocer mediante extracción de imágenes de video; Válido para qué resoluciones; Capacidad de procesar varias caras en una misma imagen; Determinación del género y expresiones faciales; Tolerancia a la traslación o rotación; Tamaño de base de datos capaz de gestionar; Premios/reconocimientos como algoritmo; Características o imperfecciones que elimina de la muestra; FRR y FAR en pruebas reales.

VeriLook [20]: Admite tanto reconocimiento 1-1 como 1-N; reconoce caras vivas mediante video por lo que poner una fotografía delante de la cámara no funciona; reconocimiento de imágenes a través de video; válido para cámaras low cost de baja resolución; procesa varias caras al mismo tiempo; capaz de determinar el género de la persona; detecta a la personas con gafas o movimientos de la boca (sonrisa, boca abierta, etc.); gestión de calidad de las muestras obtenidas y utilización de las de mejores características; tiene tolerancia a la traslación o rotación; puede gestionar una base de datos ilimitada.

Además de las FAR/FRR que veremos posteriormente, Neurotechnology cita unas recomendaciones para que la calidad de la imagen sea óptima para funcionamiento del algoritmo:

- La cámara con la que se recluta debe tener características similares a las que se usa para el reconocimiento.
- Distancia de 50 pixeles entre los ojos para reconocimiento por video y 75 pixeles entre los ojos para obtener los mejores resultados.
- Mínima resolución de imagen de 640 x 480 pixeles.
- No reclutar o verificar mediante imágenes reflejadas o modo espejo en la imagen.
- Iluminación directa difusa frontal a la cara para evitar sombras pero que no sea una luz deslumbrante para que no se refleje en gafas.
- Las tolerancias para el reconocimiento:
  - De frente o de perfil según la configuración.
  - ± 30 grados girando la cabeza o 45 grados si tenemos varias muestras de la misma persona/cara.
  - ±15 grados cambiando la inclinación de la cabeza o hasta 25 grados si tenemos varias muestras de la misma persona/cara.
- Se recomienda un reclutamiento con una expresión de cara neutra.
- Reconocimiento por video al menos a 10 FPS aunque lo recomendable es entre 10-25 FPS.
- Es recomendable moverse ligeramente durante el reconocimiento, girar la cabeza, cambiar de inclinación, etc.
- Evitar gafas de sol o gafas de cristal con una pasta muy ancha.
- Evitar mucho maquillaje.
- El cambio del bello facial o el pelo de la cabeza puede dificultar el reconocimiento.

Para juzgar la FRR y FAR Neurotechnology analiza la respuesta del algoritmo frente a diferentes situaciones. Puesto que las necesidades para la obtención de la imagen son muy comunes no hace hincapié en qué cámara usó porque las conclusiones no son sensibles a este factor, aunque si existen otros más determinantes como veremos a continuación.

Se analizarán dos experimentos: Experimento nº1 es una prueba de reconocimiento con iluminación controlada y una sola imagen (situación similar a los sistemas ABC), y el experimento nº2, es para analizar el aumento de rendimiento cuando existen 4 imágenes de la persona. Además, dentro del propio experimento se realizan dos tests, uno realizado a máxima precisión y otro, minimizando la calidad y aumentando la capacidad de procesamiento.

Además, Neurotechnology considera que el espacio de tiempo entre la foto de reclutamiento y la de identificación puede afectar de manera significativa al reconocimiento. Por ello realiza tres pruebas, una con fotos de alistamiento de hace medio año, otra con un periodo de un año y una última, con un año y medio o más.

A continuación se verá el gráfico ROC de cada experimento. Para ayudar a la interpretación se detallará sobre la correspondencia de cada trazo. La línea roja es el experimento nº1 dando más importancia a la velocidad de procesamiento que a la calidad. La línea azul es el experimento nº1 dando más importancia a la precisión. La línea morada es el experimento nº2 dando más importancia a la velocidad de procesamiento que a la calidad. La línea azul claro es el experimento número 2 dando más importancia a la precisión. La curva Receiver Operation Characteristic (ROC) se usa para demostrar la calidad de un algoritmo enfrentando FAR /FRR.

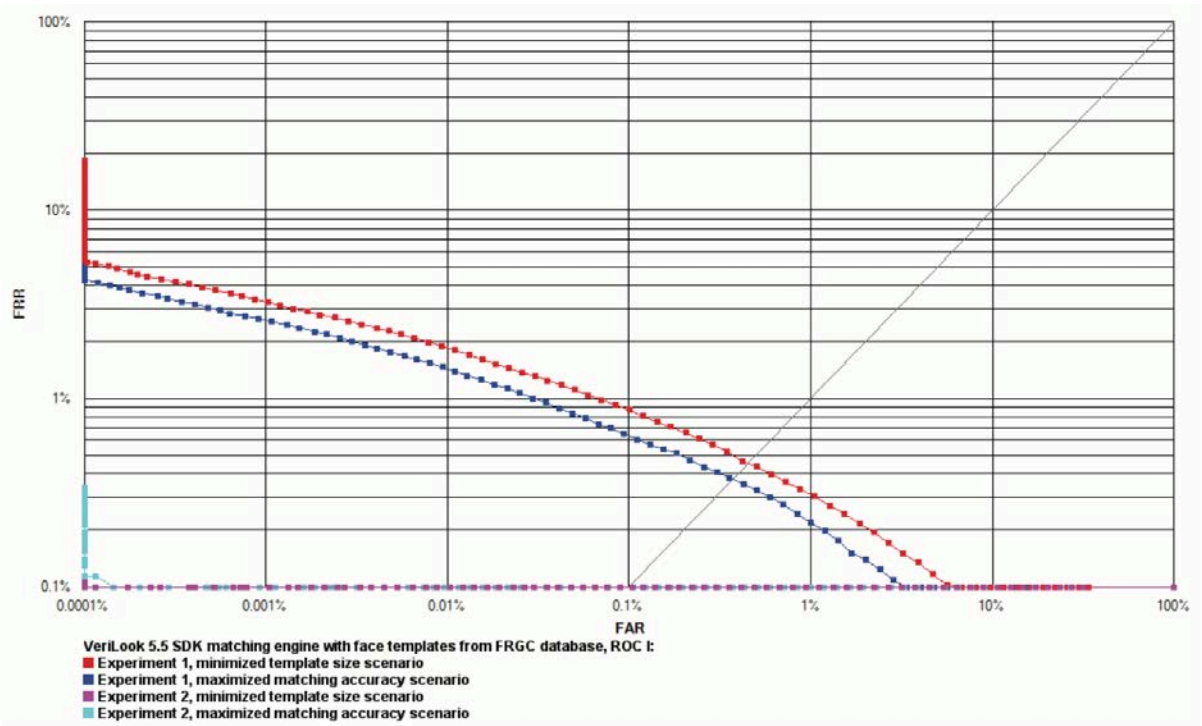


Figura 25. ROC con medio año de diferencia entre el reclutamiento y la identificación [20]

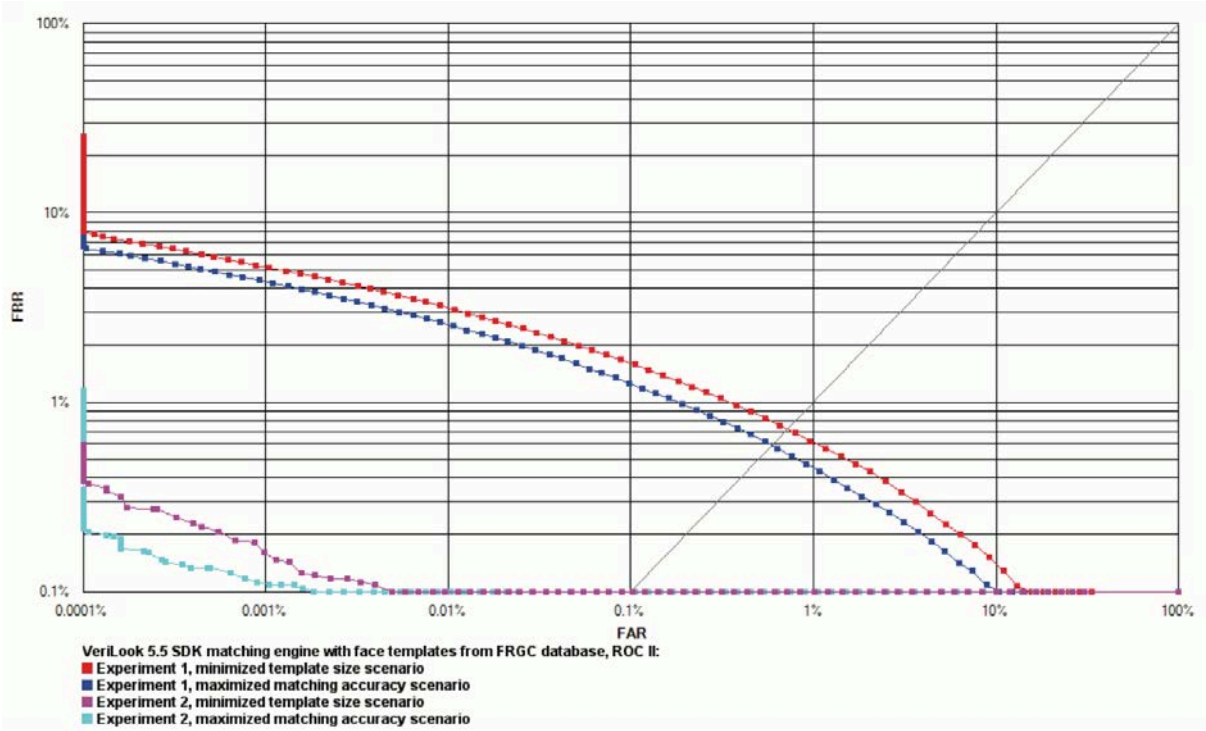


Figura 26. ROC con un año de diferencia entre el reclutamiento y la identificación [20]

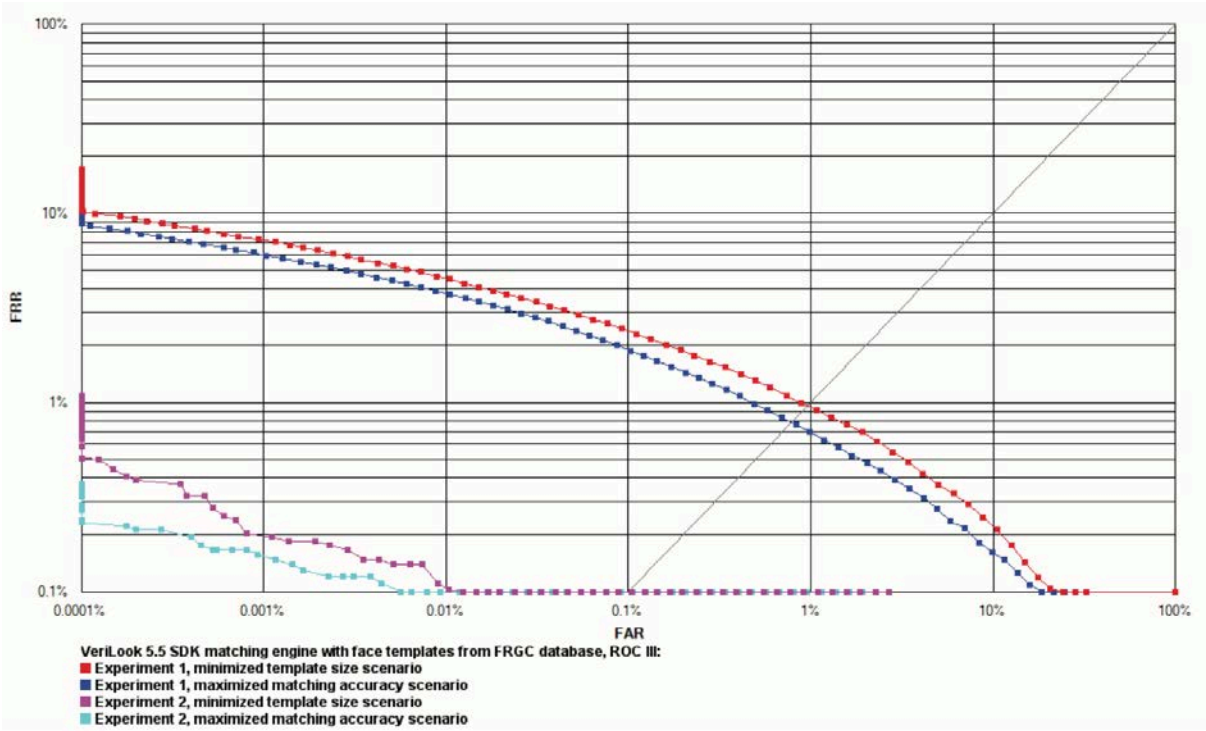


Figura 27. ROC con más de un año y medio de diferencia entre el reclutamiento y la identificación [20]

Se puede concluir que para el experimento nº1 (caso más parecido a un sistema ABC) la precisión no es muy buena teniendo unos porcentajes FAR y FRR bastante altos y sin embargo, la diferencia temporal entre el reclutamiento y la identificación apenas varía los resultados. Por otro lado, el hecho de procesar a la máxima velocidad o con precisión máxima no supone una gran diferencia, aunque para el primero sean más desfavorables los resultados.

En cuanto al experimento nº2, cuando se tiene cuatro fotos de la misma persona, entonces los porcentajes FAR y FRR descienden tremendamente, volviéndose el algoritmo mucho más efectivo. Además si que se puede observar como el periodo de tiempo entre la captura de las fotos afecta bastante a la FAR y FRR, aumentando cuanta más diferencia hay entre el reclutamiento y la identificación.

Pese a que en el mejor de los casos hubiera un FAR en torno al 10 % no es un porcentaje de éxito suficiente como para poder utilizar esa especificación del algoritmo en nuestro beneficio en un ataque Zero- Effort o Esfuerzo Cero. Se considera que para que un ataque de ese estilo sea viable deberá ser exitoso con un porcentaje considerablemente alto para que una falsa aceptación sea un evento más típico. Más adelante se volverán a usar estos resultados.

Hasta aquí llega el apartado 4.2.2 Descripción específica del sistema. Donde se ha pasado de no tener información del sistema ABC a restringir qué queremos vulnerar (reconocimiento facial y dactilar), qué sensor dactilar y qué reconocimiento facial usa (sensor óptico reflexivo y reconocimiento facial geométrico), qué vulnerabilidades tienen sus algoritmos (VeriFinger y VeriLook) así como especificaciones en tipo de sistema ABC que más conviene vulnerar y en que situaciones, saber acerca del cotejamiento de la identidad documental con las bases de señalamiento del CNP y el proceso de evaluación, entre más cosas. Con ello se adquiere un buen punto de partida para buscar ataques que puedan vulnerar el sistema ABC seleccionado.

4.2.3 Descripción de las BBDD y protocolo de evaluación

En los sistemas ABC, debido a que de su seguridad depende del control de fronteras se realizan tanto tareas de verificación del pasajero como de identificación con las principales bases de datos (BBDD) del CNP. La tarea de este apartado será determinar los procesos de reconocimiento que se llevan a cabo en el sistema ABC y definir el tipo de BBDD que usan.

Existen dos principales tipos de bases de datos para los sistemas ABC:

- Base de datos distribuida: es un sistema en el cual múltiples sitios de bases de datos están ligados por un sistema de comunicaciones de tal forma que, un usuario en cualquier sitio puede acceder los datos en cualquier parte de la red.

- Base de datos centralizada: es un sistema que almacena en su totalidad una base de datos en una sola máquina y una sola CPU, y en donde los usuarios trabajan en terminales secundarias que sólo muestran resultados.

Por un lado se realiza la tarea de verificación propiamente dicha en el sistema ABC, que coteja la muestra biométrica introducida con la base de datos, que en nuestro caso será la muestra incluida en el DNI-e. Este método de comparación se llama Match-On-Card (MoC) y elimina la necesidad de tener una BBDD centralizada puesto que, tanto el almacenamiento como el procesamiento, se hacen en la propia tarjeta, eliminando así la posibilidad de un ciberataque. Este método de almacenamiento distribuido se llama Storage-On-Card (SoC).

Por lo tanto, el primer proceso es una comparación 1-1 para demostrar si la muestra biométrica introducida realmente corresponde con la persona que dice ser.

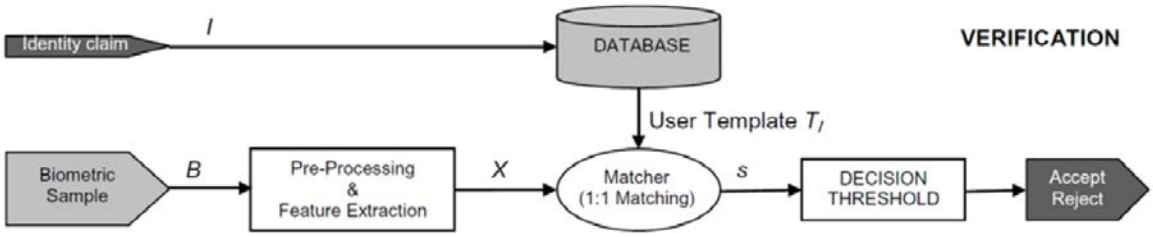


Figura 28. Proceso de verificación [5]

Por otro lado, existe la tarea de identificación que coteja la identidad con cuatro grandes BBDD centralizadas del CNP: el Sistema de Inspección de Pasaportes, el Sistema de Autenticación de DNI electrónico, las BBDD de Personas y Documentos de la Policía, y el Registro del paso de fronteras. A pesar de la falta de información debido a la naturaleza del asunto, debe existir un cotejamiento con bases de datos internacionales como listas negras para personas potencialmente peligrosas, con delitos graves o de personas buscadas por las fuerzas de seguridad.

Por lo tanto, existe una comparación 1-N de los documentos y de la muestras biométricas.

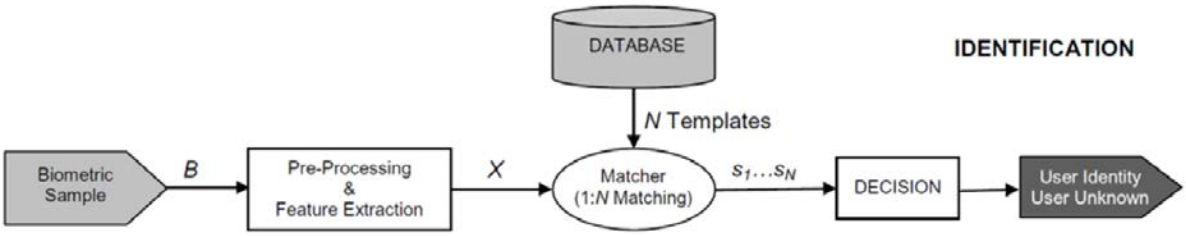


Figura 29. Proceso de identificación [5]

El esquema interno de los aeropuertos españoles con las BBDD del CNP en los sistemas ABC se organiza según el siguiente esquema:

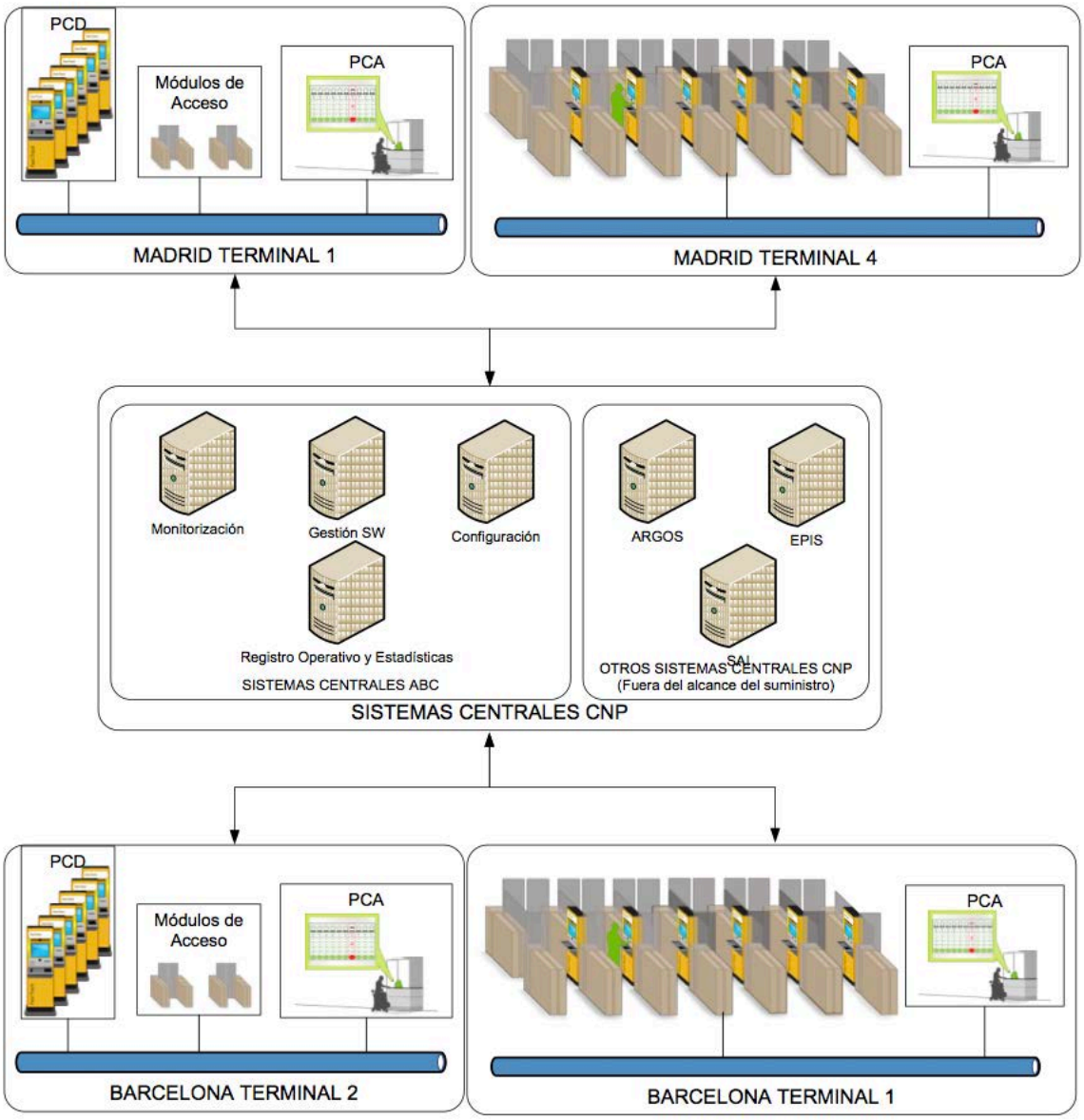


Figura 30. Esquema de conexión de las BBDD del CNP en los aeropuertos españoles [13]

4.2.4 Como vulnerar el sistema

Como se definió anteriormente, existe la posibilidad de vulnerar el sistema buscando nuevas vulnerabilidades (identificación) o simplemente explotar vulnerabilidades ya conocidas (explotación). En general, el tiempo necesario es mayor para realizar una identificación que para una explotación pero será el propio evaluador el que decida qué método quiere escoger sabiendo que tendrá una repercusión a la hora de calcular el potencial de ataque.

Puesto que la información más sensible de los sistemas ABC no es pública, se supone que el esfuerzo para identificación de vulnerabilidades es demasiado alto y por ello, se decide que el mejor método para vulnerar el sistema es mediante explotación. Los focos de atención se centrarán entonces en las vulnerabilidades de la verificación documental y en el reconocimiento facial y dactilar.

4.2.5 Condiciones del sistema y otros datos de interés

Las condiciones reales en otros casos de evaluación biométrica pueden ser irregulares por estar expuestos a condiciones más adversas. En el caso de los aeropuertos y los sistemas ABC, los sistemas de saneamiento y de ventilación están controlados para mantener unas condiciones ambientales agradables, óptimas y estables. Además, como se vio en el apartado de especificaciones técnicas el sistema está equipado con un sistema de iluminación.

Por ello, los factores de mala iluminación, muy alta o baja la temperatura y altos grados de humedad ambiente en los sistemas ABC no existirán y de modo que no se producirá un problema que incite a fallos de funcionamiento debido a las condiciones ambientales.

Otros datos de interés:

Puesto que solo existen dos aeropuertos españoles con esa tecnología (Barajas (Madrid) y El Prat (Barcelona)), sólo se podrá intentar pasar por otro usuario a través de esos sistemas ABC hacia otros aeropuertos con sistemas ABC implantados y que se encuentren dentro de la comunidad Schengen.

Además, la identidad que va a ser suplantada debe de poseer un DNI e o un pasaporte electrónico para poder usar los PCDs y el falsificador deberá conocer o averiguar la clave PIN de dichos documentos.

Por último, la edad es también un factor determinante. No puede haber diferencias grandes de edad entre el falsificador y la persona que se quiere suplantar puesto que la complexión en muchos casos no será coherente. Por ejemplo, una persona de 60 años no puede hacerse pasar por una de 12 o viceversa. Se supone un rango de edades de entre 18 y 65 años.

4.2.6 Restricción de ataques y búsqueda de información

Como se vio en la metodología de evaluación de la seguridad para sistemas biométricos, los ataques en una primera instancia se dividen en ataques Zero-Effort o cero esfuerzo y los ataques Adversary o adversario.

Los ataques cero esfuerzo se basan en los fallos del propio sistema como la FAR o FRR donde un alto porcentaje de veces un usuario es aceptado siendo realmente otro.

En los ataques adversario, realmente existe un propósito falsificador para suplantar la identidad de otra persona interviniendo en el proceso ya sea de forma directa o indirecta como se verá más adelante.

En la descripción del sistema ABC en el apartado de algoritmos, se vio que los fallos relacionados con la ROC no son tan altos como para ser significativa y poder suplantar una identidad sin esfuerzo. Además al ser un sistema multibiométrico compuesto por reconocimiento facial y dactilar complica enormemente el éxito de dos ataques Zero-Effort consecutivos. Por dicho motivo, se descartan ese tipo de ataque y se enfoca el análisis hacia los ataques Adversary o adversario.

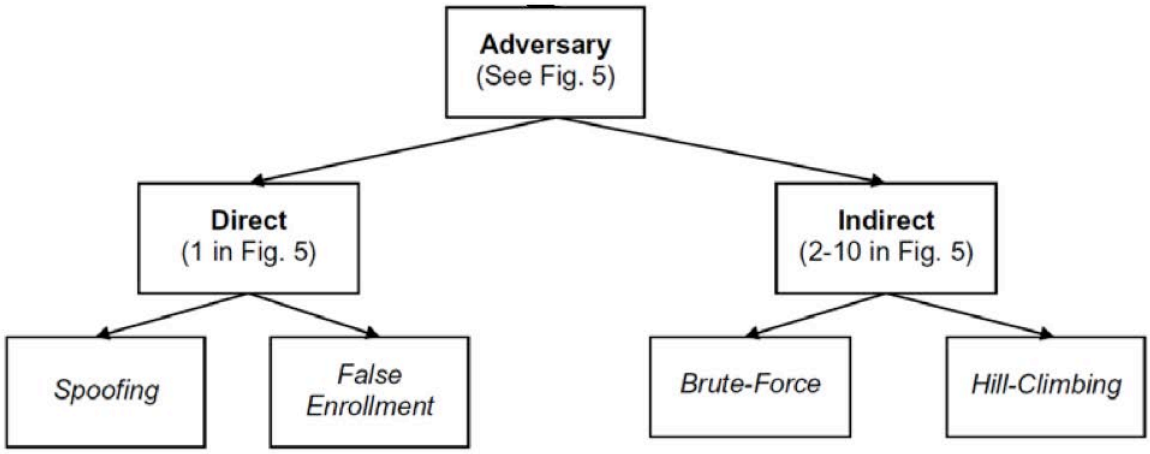


Figura 31. Clasificación de ataques adversario [9]

Los ataques Adversary se dividen en dos grupos: los ataques directos e indirectos. Como se puede observar en la siguiente figura 32 , los ataques directos se centran en falsificar la muestra biométrica introducida en el sistema para que después del procesamiento interno concuerde con la muestra de la base de datos. Por el contrario los ataques indirectos se centran en la manipulación del procesamiento de la imagen y en la base de datos. Será el propio evaluador el que seleccione que tipo de ataque que se ajuste más a sus habilidades. A pesar de todo, se darán unos ligeros esbozos de los tipos de ataques más comunes.

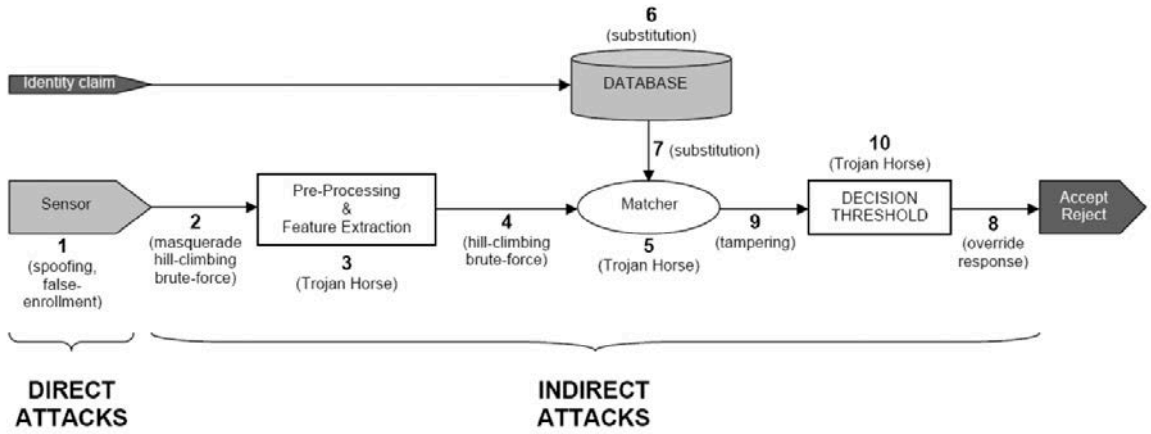


Figura 32. Puntos de aplicación de ataques adversario [9]

- Ataque directo - Spoofing: Implica sustituir completamente la identidad física con muestras biométricas falsas y copiadas de la identidad que se quiere suplantar. En el caso de los sistemas ABC españoles se haría mediante la falsificación de la huella dactilar y de la cara.
- Ataque directo - False Enrollment: Este ataque se basa en la premeditación de que en un futuro habrá personas capaces de identificarse como otra persona con las mismas muestras biométricas, sin ser falsas. Es decir, en la fase de reclutamiento o enrollment se introducen unas muestras biométricas falsas. A posteriori cualquier persona con las mismas muestras biométricas falsas pueden identificarse como ese usuario sin realmente ser un spoofing porque no está suplantando la identidad de nadie sino que se está identificando con unas muestras biométricas falsas que han sido registradas. En este caso el grado de aceptación en los sistemas es mucho mayor puesto que se está comparando una muestra falsa con una muestra falsa y no una muestra verdadera con una muestra falsa como en ataques spoofing. En el caso de los sistemas ABC españoles se haría con la huella dactilar y la fotografía.
- Ataque indirecto - Brute Force: Este ataque se basa en probar todas las posibles combinaciones hasta que coincide con la deseada. Por ejemplo, introducir todas las combinaciones posibles de un código PIN de 4 dígitos. En el caso de los sistemas ABC un ataque de fuerza bruta queda completamente descartado ya que la cantidad de variables que hay y la cantidad de posibilidades de cada una de ellas (caras y sus facciones o huella y sus características) crearían unas necesidades y unas velocidades de procesamiento que serían imposibles de conseguir.
- Ataque indirecto - Hill Climbing: Es un algoritmo iterativo que comienza con una solución arbitraria al problema, luego intenta encontrar una mejor solución variando incrementalmente un único elemento de la solución. Si el cambio produce una mejor solución, otro cambio incremental se le realiza a la nueva solución, repitiendo este proceso hasta que no se puedan encontrar mejoras. Es un ataque con mucho éxito, pero sin embargo, se vuelve a necesitar una capacidad de procesamiento muy alta y la capacidad de acceder al sistema.

Existe un problema en cuanto a los ataques indirectos y es que se necesita poder acceder al sistema informático del sistema ABC para poder manipular los datos. Estos ciber ataques ya han sido contemplados y por ello el método de identificación que se realiza es MoC lo que elimina la necesidad de una BBDD y provee más seguridad frente a ataques indirectos.

Otra clase de ataque que se podría realizar a los sistemas ABC sería lograr cambiar la información electrónica del DNI e de forma que se pudiera identificar como un usuario correctamente colocando información falsa en el chip de la tarjeta. Sin embargo, existe información la cual asegura que la clonación o modificación de los datos de DNI e no es posible debido a sus sistemas de seguridad [21].

Se debe aclarar que existen más ataques y que estos se están actualizando constantemente. Será parte del trabajo del evaluador identificar el grupo principal y catalogar el tipo de ataque a realizar.

Como se ha concluido anteriormente, los ataques indirectos quedan descartados y por ello se focalizará en los ataques directos Spoofing. También se ha descartado el False Enrollment o falso reclutamiento porque en la comisaría cuando se hace el DNI e o el Pasaporte electrónico se está asistido en todo momento por un agente, lo que imposibilita introducir una huella falsa y una cara que no corresponde con la persona que se está haciendo el documento.

En cuanto a ataques spoofing de huella y cara se tienen dos opciones de obtener las muestras biométricas: con colaboración o sin colaboración.

- Con colaboración: Como sus propio nombre indica se tiene completamente disponible a la persona que queremos a suplantar y por lo tanto, su ayuda. Conseguir muestras de su huella, fotografías de su cara y el documento de identificación no será complicado.

- Sin colaboración: En este caso, no se tendrá un acceso fácil a las muestras biométricas ni a los documentos por lo que se tendrán que obtener de forma indirecta. No obstante conseguir una fotografía o una huella es una cuestión de tiempo dado que la imagen es pública y que las huellas quedan plasmadas en la mayoría de las superficies que se tocan.

Aquí concluye la primera parte de la metodología de evaluación de la seguridad para los sistemas ABC. En esta primera fase de búsqueda de las posibles vulnerabilidades se ha descrito de forma precisa y técnica todo lo referente al sistema físico ABC y su evaluación para identificar una identidad. Una vez se ha ido acotando la información relevante, se han ido descartando diferentes tipos de ataques hasta quedarse con los más interesantes o los que se piensa que pueden tener mayor éxito. En el caso de los sistemas ABC de los aeropuertos españoles los ataques directos Spoofing.

Una vez se ha restringido la información del sistema ABC se podrán buscar ataques para sus diferentes posibles vulnerabilidades vistas en esta primera fase. Es uno de los gruesos del proceso de evaluación e intervendrá la capacidad del mismo de conseguir información relevante ya sea de artículos, revistas, libros, internet, etc.

A partir de aquí comienza la fase 2, el estudio y definición de los ataques.

4.3 Fase 2: Estudio y definición de los ataques

En esta fase se buscará una definición exacta de los ataques que se quieren realizar y que en teoría pueden vulnerar el sistema. Para ello se deberán incluir los pasos secuenciales para su ejecución, sus materiales, etc. También se hará un análisis teórico de los ataques basado en el cálculo de su potencial de ataque, que posteriormente se usará en una última fase para calcular la resistencia del TOE.

Es muy importante dedicar un gran grueso del tiempo al estudio y definición de los ataques puesto que serán los que finalmente acotarán la seguridad del sistema. Por ejemplo, si con un potencial intermedio logramos vulnerar el sistema, entonces el TOE será vulnerable frente a potenciales de ataque mayores y tendrá resistencia a ataques con menor potencial.

Este apartado servirá como ejemplo para el estudio y definición de cualquier ataque a un sistema ABC. Es por ello que esta fase estará redactada de forma muy práctica y enfocada hacia ejemplos concretos para los sistemas ABC de los aeropuertos españoles puesto que es la única forma de ejemplificar.

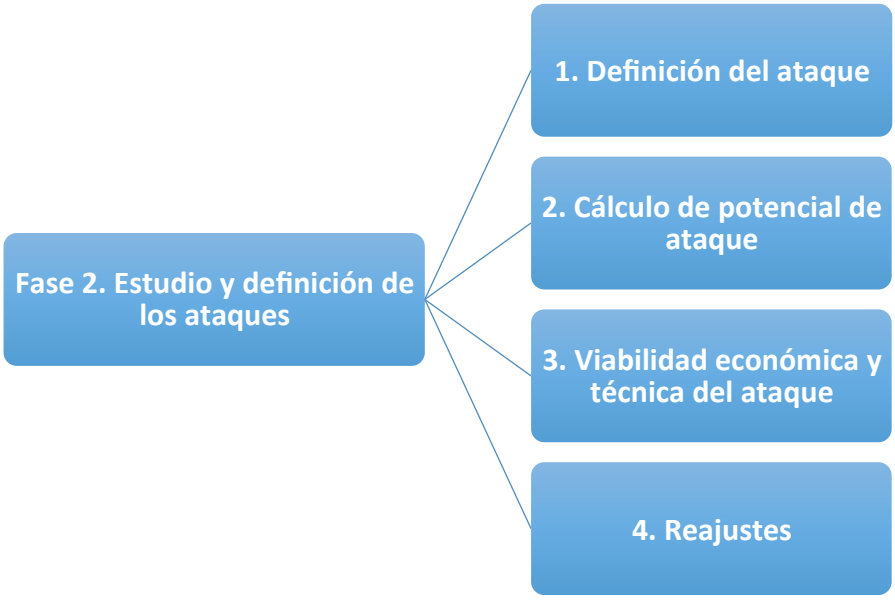


Figura 33. Esquema detallado de la fase de estudio y definición de los ataques

4.3.1 Definición del ataque

Como se vio en el apartado 3.3.1 se debe escribir una receta del ataque. Puesto que un sistema ABC es un sistema multi biométrico, se tendrán en cuenta que cada ataque estará formado por varios ataques correspondientes a cada identificación biométrica del sistema. Por ejemplo, para los sistemas ABC españoles, hará falta un ataque para el reconocimiento dactilar y otro para el reconocimiento facial.

Como se comentó anteriormente existe otra subdivisión de los ataques y es la disposición o no de la colaboración del usuario que se quiere suplantar. Por lo tanto, para ejemplificar, se definirá un ataque directo spoofing con colaboración y sin colaboración, ambos formado por un ataque de reconocimiento facial y otro dactilar.

4.3.1.1Ataque directo spoofing con colaboración

- **Ataque huella dactilar: Huella viva / Matsumoto**

Este ataque se caracteriza por su sencillez y efectividad. Un método desarrollado por Tsutomu Matsumoto basado en crear un molde mediante componentes sencillos y después realizar una copia de la huella con tan solo gelatina [22]. Como requisito especial se debe tener la colaboración de la identidad a suplantar para realizar moldes de buena calidad.

Materiales que se necesitan:

1. Persona física para copiar la huella.
2. Grazna de plástico / arcilla de dentista o pistola termoplástica.
3. Gelatina y agua (Parte 1/2 gelatina y 1/2 agua).
4. Nevera y olla.

Receta:

- 1º Crear el molde (Unos 10 minutos hasta que se seque):
  - Derretir la grazna de plástico en la olla con agua y presionar con el dedo.
  - Arcilla de dentista prepararla y presionar con el dedo.
  - Expandir el plástico caliente por una superficie y presionar con el dedo.
- 2º Preparar el material con la gelatina y el agua. Añadir en partes iguales, agua hirviendo (gr) con los mismos gramos de gelatina (planchas). (Unos 20 minutos reposando)
- 3º Vertemos la gelatina sobre el molde y lo introducimos en la nevera. (Durante unos 15 minutos).
- 4º La huella ya estará lista para usar.

Referencia: [22]

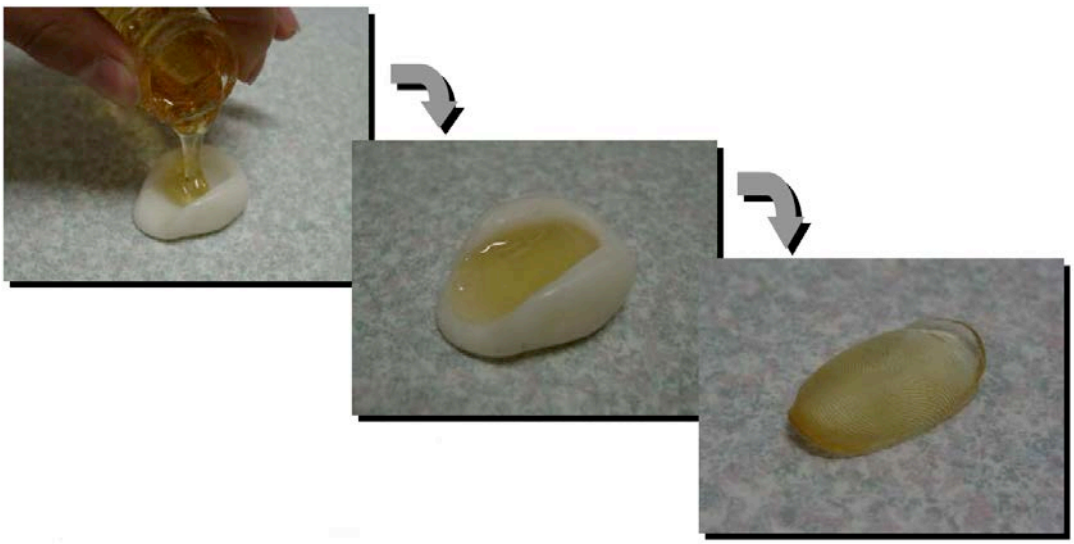


Figura 34. Método de Matsumoto [22]

- **Ataque Reconocimiento facial : Cara viva**

Este ataque se basa en el mismo concepto que el ataque de Matsumoto solo que de cara. En este caso se realizará un molde de la cara del sujeto y posteriormente se hará una máscara de látex copiando así, los rasgos físicos. Como requisito especial, aparte de tener la colaboración de la identidad a suplantar, para realizar moldes de buena calidad se debe evitar las barbas porque el acabado no es realista.

Materiales que se necesitan:

1. Yeso (No tiras de yeso porque son menos precisas y no resaltan tan bien los rasgos).
2. Agua.
3. Papel transparente de cocina.
4. Cola blanca.
5. Persona física que se quiere suplantar.
6. Crema hidratante/Vaselina.
7. Látex

Receta:

- 1º Preparar la cara para hacer el molde.
  - Poner un poco de látex / cola blanca en la frente para posteriormente recoger el pelo y con ayuda de papel transparente de cocina (Muy apretado) poder crear una superficie lisa entre la frente y el pelo.
  - Proteger el pelo facial, poniendo crema hidratante / Vaselina en las cejas, bigotes y pestañas para que el yeso no se quede pegado.
  - Preparar la mezcla de yeso.
- 2º Preparar el molde.
  - Se empieza por la nariz porque es la parte más delicada. Aplicar una cantidad generosa y moldear con los dedos la nariz. Después los ojos y el resto de la cara. Hay que asegurarse de cubrir todas las zonas presionando con las manos para evitar burbujas de aire.
  - Se debe hacer una capa bastante gruesa y una vez esté expandida toda la cara se tiene que dejar secar un poco para luego aplicar las láminas de yeso. Se mojan en agua las láminas de yeso y se ponen por la cara haciendo el mismo recorrido que en el paso anterior, es decir, por la nariz, ojos y luego el resto de la cara. Hay que asegurarse de apretar para que no queden relieves sin cubrir. Como se quiere hacer un molde muy sólido para luego crear copias se necesitarán al menos 10 capas de yeso en láminas.
  - Una vez esté seco quitar el molde de la cara.
- 3º Creando la copia de la cara.
  - Una vez se tenga el molde solo se tiene que verter el látex.
- 4º Pintar las cejas, labios, y puntos característicos para que la cámara lo detecte (para un mejor resultado se puede acudir a un especialista).
- 5º La copia está lista para usar.

Referencia: [23]

Figura 35. Creando molde cara viva [23]

Figura 36. Máscara creada a partir del molde [23]

4.3.1.2 Ataque directo spoofing sin colaboración

- **Ataque de huella dactilar: Huella latente / No viva**

Este ataque se caracteriza porque no se tiene colaboración por parte de la persona que se quiere suplantar y por lo tanto, el acceso a sus muestras biométricas es mucho más complicado. Sin embargo, esta persona no puede ser completamente desconocida puesto que se necesita robar un documento de identificación y se debe de tener cierta información como los sitios que frecuenta para poder obtener sus huellas (Vaso de un restaurante, el pomo de una puerta, etc.). En general, las muestras obtenidas por métodos sin colaboración tienen peor calidad.

Materiales que se necesita:

1. Polvo de fotocopiadora (tóner).
2. Brocha de maquillaje suave, cuanto más fino sea el pelo mejor.
3. Buena cámara con macro (iPhone con lente macro o cámara réflex).
4. Programa de manipulación de imágenes (Tipo Photoshop).
5. Papel de transparencias e impresora de alta calidad (Una reprografía).
6. Barniz/Pintura foto sensitiva (Positiv 20 by Kontakt Chemie).
7. Bombillas de rayos UV o bombilla normal en su defecto.
8. Placa de cobre para circuito impreso.
9. NaOH (Sosa cáustica), es decir, lejía.
10. FeCl3 (Cloruro de hierro III). Se puede comprar en internet fácilmente.
11. Pincel.
12. Gelatina y agua a partes iguales.
13. Nevera y olla .
14. Agua.

Receta:

- 1º Obtener la huella:
  - Seguir a la persona y esperar a que ponga las manos en algún objeto, si es una superficie plana y horizontal mejor.
  - Se echa encima el polvo de tóner generosamente y después con la brocha de maquillaje se quita poco a poco el exceso hasta que se quede la huella.
  - Hacer una foto de alta resolución a la huella. Además se debe medir la distancia entre los dos puntos característicos de la huella (distancia entre el Core y Delta) para escalar debidamente con el programa de edición de foto y así imprimir con el mismo tamaño que la huella real.
- 2º Hacer la transparencia para la PCB:
  - Se edita la foto con el programa de edición de fotos. Se quita el polvo sobrante y completan las grietas en la huella para crear uniformidad.
  - Aumentar el contraste para crear un patrón muy claro en la huella.

- Escalar la imagen a la realidad (Con la distancia de Core y Delta que se midió).
- Se invierte la imagen para crear un negativo y se imprime en papel transparente.

- 3º Hacer el molde:

  - Aplicar el barniz/pintura foto sensible en la placa de cobre y dejar secar.
  - Pegar la transparencia de la huella con celo a la PCB.
  - Aplicar luz UV durante 10-15 minutos o bien 30 minutos con una bombilla normal.
  - Quitar la transparencia.
  - Usar la lejía para quitar el barniz foto sensitivo, o bien con el pincel para tener más precisión o metiéndolo en un recipiente con lejía y agitando hasta que se desprenda.
  - Echar el cloruro de hierro III (FeCl3) y verter sobre la placa hasta que se quede la huella en la PCB.
  - Lavar con agua y después pasar con un trapo alcohol.
  - Verter la mezcla de gelatina con agua (50-50) encima de la PCB y meter en la nevera.

- 4º La huella ya estará lista para usar.

Referencia: [24]

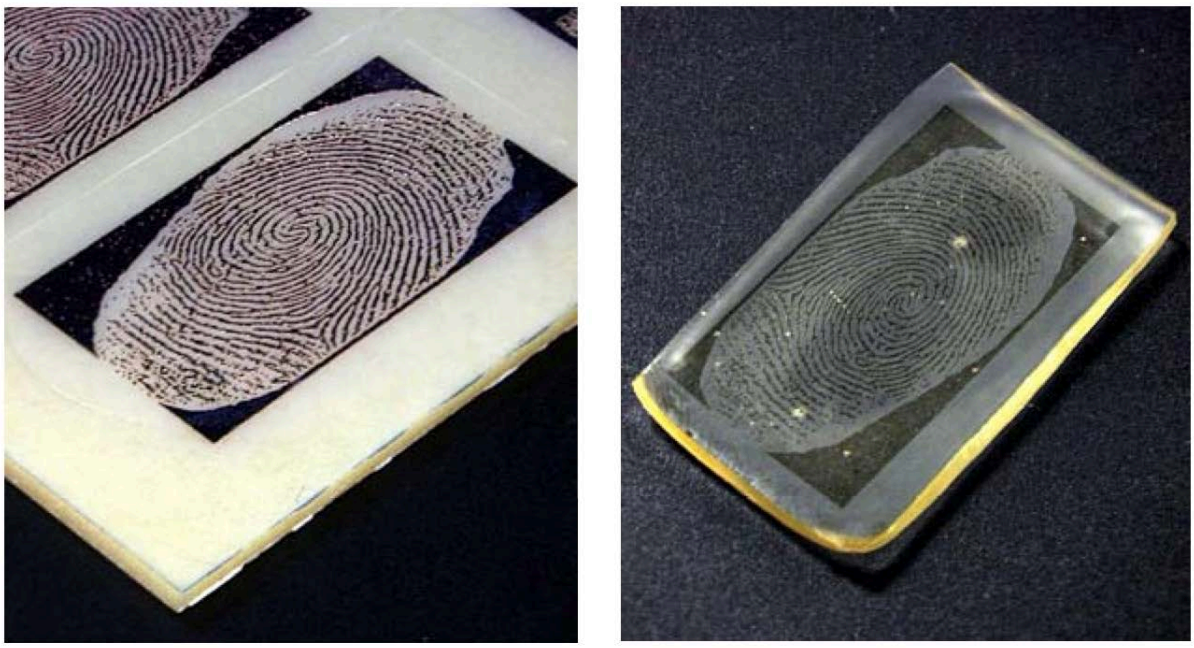


Figura 37. Método por huella latente [24]

- **Ataque de reconocimiento facial : Cara no viva**

Este ataque se basa en la creación de una máscara a través de una foto de perfil y una foto frontal de la cara. Es un proceso experimental que aún no ha sido testado pero en teoría, puesto que los algoritmos se fijan en unos puntos característicos de la cara, si fuéramos capaces de recrear esos mismos puntos (las distancias entre ellos) se conseguiría una cara idéntica a ojos de reconocimiento facial.

Este ataque se caracteriza porque no se tiene colaboración por parte de la persona que se quiere suplantar y por lo tanto, el acceso a su muestra biométrica facial es mucho más complicado. Sin embargo, esta persona no puede ser completamente desconocida puesto que se necesita robar un documento de identificación y se debe de tener cierta información como los sitios que frecuenta para poder obtener una foto de dicha persona. En general, las muestras obtenidas por métodos sin colaboración tienen peor calidad.

Materiales que se necesitan:

- Cámara fotográfica

Receta:

1. Sacar fotos de los 2 perfiles y de frente.
2. Enviar las fotos a ThatsMyFace.
3. Recibir la máscara y listo para usar.

Referencia: [25]

Figura 38. Thatsmyface muestra de máscara [25]

4.3.2 Cálculo de potencial de ataque

Como se vio en el apartado 3.3.2 una vez se ha definido el ataque, el paso inminente es el cálculo de potencial de ataque en base a cinco factores:

- **Tiempo necesario para identificar y desarrollar el ataque** (**Elapsed Time**): Es el tiempo total necesario para que el atacante o evaluador identifique una posible vulnerabilidad en el TOE, incluyendo el tiempo de desarrollo del ataque y su ejecución.

- **Requerimientos técnicos específicos** (**Specialist Expertise**): Se refiere al nivel de conocimiento específico de los principios básicos del sistema (protocolos, sensores, etc.), del producto o de métodos de ataque.

- **Conocimiento del TOE** (**Knowledge of the TOE**): Se refiere al nivel de información especializada a la que puede acceder en relación al TOE.

- **Oportunidades** (**Window of opportunity**): Es uno de los factores determinantes y engloba las oportunidades para enfrentarse al sistema medido en tiempo de acceso y en número de intentos que se pueden realizar. En muchas ocasiones este factor es el que impide la realización de un ataque porque no es posible llevarlo a cabo debido a que se necesita mucho tiempo para hacer pruebas o muchos intentos para probarlo.

- **Equipo necesario** (**IT hardware/software or other equipment**): Se refiere al equipo requerido para identificar o explotar una vulnerabilidad.

Utilizando la clasificación de cada factor y con los pesos de cada uno en base a la Tabla 1 se calcula el potencial de ataque como:

Potencial de ataque = Valor (Elapsed time) + Valor (Specialist expertise) + Valor (Knowledge of TOE) + Valor (Window of opportunity) + Valor (Hardware/software or other equipment)

Valor	Potencial de ataque	Nivel AVA_VAN
0-9	Potencial básico	AVA_VAN.1 / AVA_VAN.2
10-13	Potencial Intermedio	AVA_VAN.3
14-19	Potencial Moderado	AVA_VAN.4
20-24	Potencial Avanzado	AVA_VAN.5
25 o más	Potencial Profesional	Más AVA_VAN.5

Tabla 3. Clasificación de potencial de ataque

4.3.2.1 Cálculo de potencial de ataque con colaboración

- **Cálculo potencial de ataque de huella dactilar: Huella viva / Matsumoto**

Para calcular dicho potencial se deben tener en cuenta los siguientes factores:

- Tiempo necesario para identificar y desarrollar el ataque (**Elapsed Time**): La búsqueda de esta información duró apenas unos días, por lo tanto, se clasifica en el grupo menor o igual a una semana correspondiente a un valor = 1.
- Requerimientos técnicos específicos (**Specialist Expertise**): Nivel de ignorante es suficiente para realizar el ataque puesto que no se necesitan conocimientos técnicos. Este nivel corresponde a un valor = 0.
- Conocimiento del TOE (**Knowledge of the TOE**): Conocimiento adquirido a través de información en internet, se clasifica en el grupo Público correspondiente a un valor = 0.
- Oportunidades (**Window of opportunity**): Se puede acceder al sensor siempre y cuando se esté pasando entre fronteras, por lo tanto no es ilimitado pero tampoco es muy limitado, se selecciona un nivel fácil de acceso lo que corresponde a un valor = 1.
- Equipo necesario (**IT hardware/software or other equipment**): La lista de componentes es estándar, por lo que los materiales no serán difíciles de conseguir, corresponde con un valor = 1.

Factor	Valor
Tiempo transcurrido	1
Experiencia especialista	0
Conocimiento del objetivo	0
Ventana de oportunidad	1
Equipamiento	1
TOTAL	3

Tabla 4. Calculo de potencial para ataque de reconocimiento dactilar con colaboración

Potencial de ataque entre 0-9 que corresponde a un **nivel Básico (AVA_VAN.1 y AVA_VAN.2)**.

Esto significa que si el ataque lograra vulnerar el reconocimiento biométrico de huella el sistema tendría una resistencia nula frente a ataques y por lo tanto sería posible suplantar una identidad siempre que el ataque tenga un potencial igual o mayor que básico, es decir, Básico (AVA_VAN.1 y AVA_VAN.2), Intermedio (AVA_VAN.3), Moderado (AVA_VAN.4), Avanzado (AVA_VAN.5) y Profesional.

- **Cálculo potencial de ataque reconocimiento facial : Cara viva**

Para calcular dicho potencial se deben tener en cuenta los siguientes factores:

- Tiempo necesario para identificar y desarrollar el ataque (**Elapsed Time**): La búsqueda de la información duró apenas unos días pero la realización del ataque entre conseguir los materiales y ejecutarlo puede llevar entre 1 o 2 semanas, lo correspondiente a un valor = 2.
- Requerimientos técnicos específicos (**Specialist Expertise**): Nivel hábil es el necesario para poder llevar el ataque ya que se requieren conocimientos específicos. Este nivel corresponde a un valor = 3.
- Conocimiento del TOE (**Knowledge of the TOE**): Conocimiento adquirido a través de información en internet, se clasifica en el grupo Público correspondiente a un valor = 0.
- Oportunidades (**Window of opportunity**): Debido a que se llevara una máscara, se considera que el posible acceso al sistema no puede ser ilimitado o si quiera una vez al día porque levantaría sospechas y pondría en riesgo la verdadera identidad. Es muy probable que de ser descubierto intentando falsificar una identidad esa misma ya no pueda seguir siendo usada y por lo tanto, el ataque de nuevo sería no válido. Se selecciona un nivel moderado de acceso lo que corresponde a un valor =4.
- Equipo necesario (**IT hardware/software or other equipment**): La lista de componentes es especializada, pese a que los materiales no puedan ser especialmente complicados de conseguir si que requiere de mucho trabajo y la necesidad de profesionales para que pueda suplantar una identidad, corresponde con un valor=4.

Factor	Valor
Tiempo transcurrido	2
Experiencia especialista	3
Conocimiento del objetivo	0
Ventana de oportunidad	4
Equipamiento	4
TOTAL	13

Tabla 5. Cálculo de potencial para ataque de reconocimiento facial con colaboración

Potencial de ataque entre 10-13 que corresponde a un **nivel Intermedio (AVA_VAN.3)**.

Esto significa que si el ataque lograra vulnerar el reconocimiento biométrico facial el sistema tendría una resistencia frente a ataques de potencial básico (AVA_VAN.1 y AVA_VAN.2) y fallo frente a ataques de potencial Intermedio (AVA_VAN.3), Moderado (AVA_VAN.4), Avanzado (AVA_VAN.5) y Profesional.

4.3.2.2 Cálculo de potencial de ataque sin colaboración

- **Cálculo potencial de ataque de huella dactilar: Huella latente / No viva**

Para calcular dicho potencial se deben tener en cuenta los siguientes factores:

- Tiempo necesario para identificar y desarrollar el ataque (**Elapsed Time**): La búsqueda de esta información duró apenas unos días pero la realización del ataque entre conseguir los materiales y ejecutarlo puede llevar entre 1 o 2 semanas, lo correspondiente a un valor = 2.
- Requerimientos técnicos específicos (**Specialist Expertise**): Nivel hábil es el necesario para poder llevar el ataque ya que se requieren conocimientos específicos para llevarlo a cabo. Este nivel corresponde a un valor = 3.
- Conocimiento del TOE (**Knowledge of the TOE**): Conocimiento adquirido a través de información en internet, se clasifica en el grupo Público correspondiente a un valor = 0.
- Oportunidades (**Window of opportunity**): Se puede acceder al sensor siempre y cuando se esté pasando entre fronteras, por lo tanto no es ilimitado pero tampoco es muy limitado, se selecciona un nivel fácil de acceso lo que corresponde a un valor =1.
- Equipo necesario (**IT hardware/software or other equipment**): La lista de componentes es especializada, pese a que los materiales no puedan ser especialmente complicados de conseguir si que requiere de mucho trabajo y de muchos materiales, corresponde con un valor = 4.

Factor	Valor
Tiempo transcurrido	2
Experiencia especialista	3
Conocimiento del objetivo	0
Ventana de oportunidad	1
Equipamiento	4
TOTAL	10

Tabla 6. Cálculo de potencial para el ataque de reconocimiento dactilar sin colaboración

Potencial de ataque entre 10-13 que corresponde a un **nivel Intermedio (AVA_VAN.3)**.

Esto significa que si el ataque lograra vulnerar el reconocimiento biométrico dactilar el sistema tendría una resistencia frente a ataques de potencial básico (AVA_VAN.1 y AVA_VAN.2) y fallo frente a ataques de potencial Intermedio (AVA_VAN.3), Moderado (AVA_VAN.4), Avanzado (AVA_VAN.5) y Profesional.

- **Cálculo potencial de ataque reconocimiento facial : Cara no viva**

Para calcular dicho potencial se deben tener en cuenta los siguientes factores:

- Tiempo necesario para identificar y desarrollar el ataque (**Elapsed Time**): La búsqueda de esta información duró apenas unos días pero la realización del ataque entre conseguir los materiales y ejecutarlo puede llevar un tiempo menor a 2 meses y mayor que 1, lo correspondiente a un valor = 7.
- Requerimientos técnicos específicos (**Specialist Expertise**): Nivel de ignorante es suficiente para realizar el ataque puesto que no se necesitan conocimientos técnicos. Este nivel corresponde a un valor = 0.
- Conocimiento del TOE (**Knowledge of the TOE**): Conocimiento adquirido a través de información en internet, se clasifica en el grupo Público correspondiente a un valor = 0.
- Oportunidades (**Window of opportunity**): Debido a que se llevara una máscara, se considera que el posible acceso al sistema no puede ser ilimitado o si quiera una vez al día porque levantaría sospechas y pondría en riesgo la verdadera identidad. Es muy probable que de ser descubierto intentando falsificar una identidad esa misma ya no pueda seguir siendo usada y por lo tanto, el ataque de nuevo sería no válido. Se selecciona un nivel moderado de acceso lo que corresponde a un valor =4.
- Equipo necesario (**IT hardware/software or other equipment**): La lista de componentes es estándar, por lo que los materiales no serán difíciles de conseguir, corresponde con un valor=1.

Factor	Valor
Tiempo transcurrido	7
Experiencia especialista	0
Conocimiento del objetivo	0
Ventana de oportunidad	4
Equipamiento	1
TOTAL	12

Tabla 7. Cálculo del potencial para el ataque de reconocimiento facial sin colaboración

Potencial de ataque entre 10-13 que corresponde a un **nivel Intermedio (AVA_VAN.2)**.

Esto significa que si nuestro ataque lograra vulnerar el sistema de reconocimiento biométrico de huella el sistema tendría una resistencia frente a ataques de potencial básico (AVA_VAN.1 y AVA_VAN.2) y fallo frente a ataques de potencial Intermedio (AVA_VAN.3), Moderado (AVA_VAN.4), Avanzado (AVA_VAN.5) y Profesional.

4.3.2.3 Cálculo de potencial total del sistema

Como es un sistema multi biométrico el ataque al sistema es el conjunto de dos ataques, uno de reconocimiento facial y uno de reconocimiento dactilar se deberá aplicar una nueva regla a la valoración del conjunto del sistema.

Se ha considerado que cuando un ataque a un sistema multi biométrico tiene diferentes potenciales se superpondrá el potencial más alto como potencial total del ataque y en caso de que ambos ataques tengan el mismo potencial, entonces se aumentará un nivel.

Es decir, como se puede ver en la tabla 7. El ataque con colaboración de huella tiene un potencial básico y el ataque de reconocimiento facial un nivel intermedio, por lo que en conjunto, tiene un nivel total intermedio.

En el caso del ataque sin colaboración, puesto que los dos tienen un nivel intermedio el nivel total de potencial de ataque será moderado.

Potencial	Huella	Cara	TOTAL
Con colaboración	3 - Básico	13 - Intermedio	Intermedio
Sin colaboración	10 - Intermedio	12 - Intermedio	Moderado

Tabla 8. Clasificación del potencial total del sistema

De esta forma se puede valorar el hecho de que sea multi biométrico ya que no es lo mismo tener que vulnerar sólo un proceso de identificación, que varios como en el sistema ABC.

4.3.3 Viabilidad económica y técnica de los ataques

Antes de entrar en profundidad en los pasos a seguir en esta fase de penetración habrá que valorar de las limitaciones que puede llegar a tener un cierto ataque para ser ejecutado en base a factores que hasta ahora no habían sido considerados. Para ello se realizará un estudio de viabilidad económica y técnica.

En el estudio se debe valorar si como evaluador, es posible realizar el ataque, ya que no vale definir ataques y estudiarlos si luego no se pueden poner en práctica. Será aquí cuando se analicen dichos factores.

Existen factores determinantes como puede ser que la ventana de oportunidad sea nula y por lo tanto no se pueda vulnerar el sistema porque no se tiene acceso a él. También podría darse el caso de que el material necesario para ejecutar el ataque no se pueda conseguir ya sea porque sea material muy restringido o porque su coste es demasiado alto.

Se debe analizar si el ataque es rentable desde el punto de vista del atacante o evaluador en este apartado. Además se añadirá el punto de vista del receptor del ataque que hasta ahora no había sido contemplado.

Desde el punto de vista del atacante la inversión de realizar todo este estudio y ejecución debe de ser rentable como principio básico al beneficio que se pretende conseguir vulnerando el sistema. En caso de no ser así, generalmente no se llegará a ejecutar por su índice de rentabilidad negativo.

En el caso del receptor del ataque, una vez se demuestra que el ataque puede vulnerar su sistema tiene dos opciones, mejorar o no el sistema. Es posible que desde un punto de vista económico sea más rentable que sea vulnerable puesto que las pérdidas por un posible ataque son menores que la inversión para actualizar el sistema frente a la amenaza.

Dicho esto, se descartan los ataques sin colaboración anteriormente planteados puesto que no se dispone de los medios físicos ni económicos para su ejecución.

En cuanto a los ataques con colaboración se hará una ligera modificación al ataque de reconocimiento facial puesto que el propósito de este documento es ilustrar como evaluar la seguridad de un sistema ABC no como vulnerarlo. Por lo tanto, ha habido un reajuste debido a la viabilidad económica y técnica de los ataques lo cual se contemplará en el siguiente apartado.

4.3.4 Reajustes

Como anteriormente se hizo una viabilidad, es posible que después de definir y estudiar el ataque resultara no ser viable para el evaluador. Es por ello que en este apartado se reajusta cualquier parte referente a los ataques, ya sea modificar los ya existentes o incluir unos nuevos con su correspondiente estudio. Puesto que se hizo un cambio, ahora se va a definir y a calcular el nuevo potencial de ataque.

Definición del nuevo ataque de reconocimiento facial con colaboración:

- **Ataque de reconocimiento facial : Cara viva / Fotografía**

Este ataque se basa en la creación de una imagen a partir de una foto frontal de la persona. Dicha imagen será impresa en distintos objetos y usada para identificarse ante la cámara de reconocimiento.

Materiales que se necesitan:

-Cámara fotográfica
-Impresora

Receta:

1. 1º Sacar una foto frontal con buena iluminación y resolución.
2. 2º La foto está lista para usar.

Figura 39. Muestra de fotografía

- **Cálculo potencial de ataque reconocimiento facial : Cara viva / Fotografía**

Para calcular dicho potencial se deben tener en cuenta los siguientes factores:

- Tiempo necesario para identificar y desarrollar el ataque (**Elapsed Time**): La búsqueda de esta información duró apenas unos días, por lo tanto, se clasifica en el grupo menor o igual a una semana correspondiente a un valor = 1.

- Requerimientos técnicos específicos (**Specialist Expertise**): Nivel de ignorante es suficiente para realizar el ataque puesto que no se necesitan conocimientos técnicos. Este nivel corresponde a un valor = 0.

- Conocimiento del TOE (**Knowledge of the TOE**): Conocimiento adquirido a través de información en internet, se clasifica en el grupo Público correspondiente a un valor = 0.

- Oportunidades (**Window of opportunity**): Debido a que se llevará una fotografía, se considera que el posible acceso al sistema no puede ser ilimitado o ni siquiera una vez al día porque levantaría sospechas y pondría en riesgo la verdadera identidad. Es muy probable que de ser descubierto intentando falsificar una identidad, esa misma ya no pueda seguir siendo usada y por lo tanto, el ataque de nuevo sería no válido. Se selecciona un nivel moderado de acceso lo que corresponde a un valor =4.

- Equipo necesario (**IT hardware/software or other equipment**): La lista de componentes es estándar, por lo que los materiales no serán difíciles de conseguir, corresponde con un valor=1.

Factor	Valor
Tiempo transcurrido	1
Experiencia especialista	0
Conocimiento del objetivo	0
Ventana de oportunidad	4
Equipamiento	1
TOTAL	6

Tabla 9. Cálculo de potencial para el ataque de reconocimiento facial reajustado

Potencial de ataque entre 0-9 que corresponde a un **nivel Básico (AVA_VAN.1 y AVA_VAN.2)**.

Esto significa que si el ataque logrará vulnerar el reconocimiento biométrico de huella el sistema tendría una resistencia nula frente a ataques y por lo tanto sería posible suplantar una identidad siempre que el ataque tenga un potencial igual o mayor que básico, es decir, Básico (AVA_VAN.1 y AVA_VAN.2), Intermedio (AVA_VAN.3), Moderado (AVA_VAN.4), Avanzado (AVA_VAN.5) y Profesional.

Finalmente el potencial de ataque del conjunto de ataques con colaboración para reconocimiento dactilar y facial es:

Potencial	Huella	Cara	TOTAL
Con colaboración	3 - Básico	6 - Básico	Intermedio

Tabla 10. Cálculo de potencial de ataque total reajustado

Una vez se ha decidido finalmente que ataques se van a ejecutar para después catalogar la resistencia del TOE será entonces cuando se pase a la tercera y última fase: La penetración o pruebas.

4.4 Fase 3: Penetración o pruebas

Durante esta fase, lo apropiado es probar todos los ataques posibles para dividirlos posteriormente en ataques que han tenido éxito y cuáles no, de forma que se pueda catalogar la seguridad del sistema y su resistencia. En este caso debido a la falta de medios se van a realizar las pruebas con el material disponible en el laboratorio que servirá como ejemplo para realizar futuras evaluaciones en sistemas biométricos o sistemas ABC.

Los apartados de esta tercera y última fase son: 1. Ejecución de las pruebas (facial y dactilar) y 2. Cálculo de resistencia del TOE.

4.4.1 Pruebas

Anteriormente en la fase 2 se definieron los ataques y se aproximó a un potencial de ataque. En la fase de pruebas se tienen nuevos interrogantes como cuántas pruebas se deberían hacer, con cuántas muestras, cuántos intentos, etc. Y aquí depende de la aplicación del sistema para aplicar uno de los dos puntos de vista de los resultados: Desde la seguridad y desde la biometría.

Desde el punto de vista de la seguridad, con que un ataque logre vulnerar el sistema una sola vez, implica que dicho sistema es vulnerable y por lo tanto, no seguro. Por otro lado, el punto de vista de la biometría se centra más en el porcentaje de éxito de dicho ataque, y generalmente debe ser un porcentaje alto, por lo tanto no vale solo una vez, sino que de forma generalizada vulnere el sistema.

Será decisión del propio evaluador dependiendo del sistema que quiera vulnerar, el aplicar uno de los dos puntos de vista. Si por ejemplo, de la seguridad del sistema depende algo tremendamente importante como un control de fronteras, sería conveniente utilizar el punto de vista de la seguridad mientras que si estamos evaluando la calidad de un sensor en particular en laboratorio, interesará más un punto de vista biométrico.

En la mayoría de los casos aplicar la estadística para sacar conclusiones del ataque suele ser inviable económicamente, por ello se usa una población de pruebas mucho más pequeña de lo que la estadística dictamina para que un resultado sea significativo. Se decidieron unas reglas para aplicar a las pruebas y así tener muestras unos resultados aceptables.

- Punto de vista de la seguridad: Se obtiene una valoración imprecisa de éxito de un ataque ya que no interesan porcentajes sino, si es posible vulnerar o no el sistema. Se ha determinado que si el ataque tiene éxito en alguna ocasión, el sistema es vulnerable.
- Punto de vista de la biometría: Se obtiene una valoración más precisa del porcentaje de éxito de un ataque determinado. Se ha determinado que si el ataque tiene un éxito de al menos un 50%, el sistema es vulnerable.

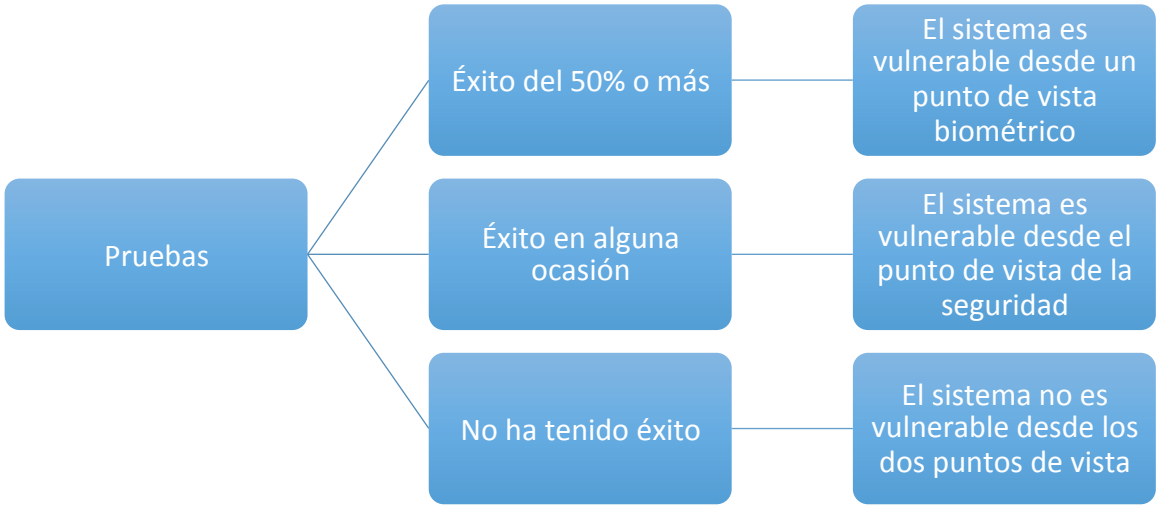


Figura 40. Clasificación de los puntos de vista de la vulnerabilidad de un sistema biométrico

Las fases para realizar una valoración crítica del éxito de un ataque son:

- 1º Fase: Obtener las muestras biométricas falsas
  - Decidir el número de usuarios para realizar el estudio:

    Se necesitarán usuarios que representen a la población que generalmente usa el sistema. Los factores que pueden afectar al estudio suelen ser la edad y sexo.

    En caso de que lo usen personas del mismo sexo y rango de edad solo se necesitarán 2 usuarios y si existen distintos sexos, pero todos tienen el mismo rango de edad, entonces se necesitarán 4 usuarios, 2 varones y 2 mujeres. Por ejemplo, si en una oficina un sistema biométrico sólo es usado por hombres de entre 35-44 años, entonces sólo se necesitan 2 varones para realizar las pruebas. Si en cambio el mismo sistema fuera usado por mujeres y varones del mismo rango de edad, entonces se necesitaría 4 usuarios, 2 varones y 2 mujeres.

    Si la edad es un factor, se considerarán diferentes rangos: entre 0-15 años, 16-24 años, 25-34 años, 35-44 años, 45-54 años y más de 55 años. Por cada rango de edad, se deben realizar pruebas con 2 hombres y 2 mujeres. Por lo tanto, el número de usuarios será igual al número de rangos de edad que abarca el sistema multiplicado por 4 (mitad mujeres y mitad hombres).

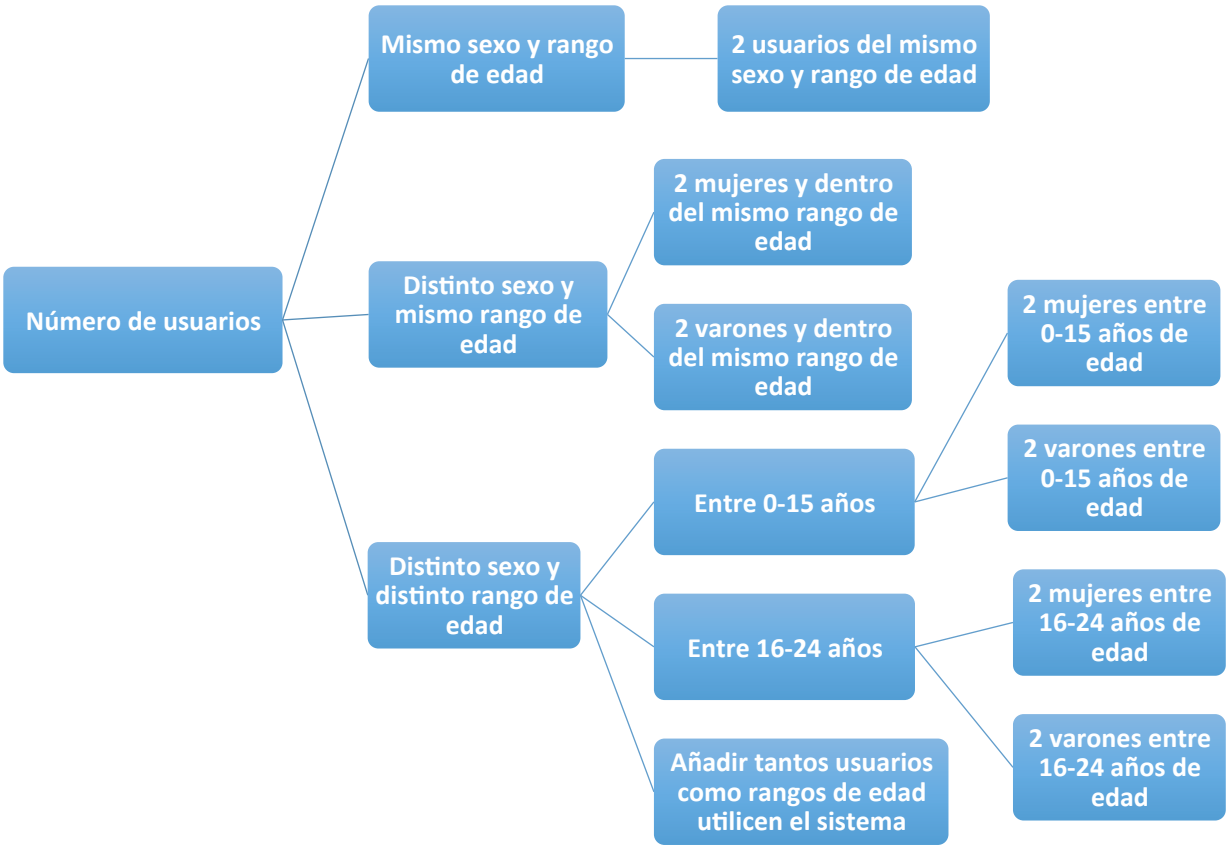


Figura 41. Selección de número de usuarios para realizar pruebas

En el caso del sistema ABC español, puesto que abarca todos los sexos y todas las edades se necesitarán 12 mujeres y 12 varones, lo que corresponde a 2 mujeres y 2 varones de cada rango de edad.

- Para cada usuario, realizar 3 muestras biométricas falsas de cada rasgo biométrico aplicando las recetas anteriormente definidas. Por lo tanto, el número de muestras que se probarán conseguirán será el número de usuarios multiplicado por 3 y todo ello multiplicado por el número de rasgos biométricos del sistema.

  En el caso del sistema ABC español que es multi biométrico y necesitan dos rasgos biométricos (Huella y cara) por cada usuario. La cuenta final considerando los 24 usuarios, por 3 muestras de cada rasgo biométrico hace un total de 144 muestras biométricas falsas (72 de cara y 72 de huella).

• 2ºFase: Comprobar la calidad de las muestras falsas obtenidas

- Inspección visual es el método más sencillo de comprobar visualmente la calidad de la muestra. Sin embargo dependerá del tipo de rasgo biométrico falsificado los puntos donde fijarse para comprobar dicha calidad. Con esta inspección se pueden descartar las muestras de peor calidad que claramente no van a servir.

  En el caso del sistema ABC bajo evaluación, la muestra dactilar puede ser sencillamente comprobada observando si los puntos característicos (Core y Delta) son visibles, que la huella está bien definida y que la muestra contiene un alto porcentaje de la superficie de la muestra real. Adicionalmente comprobar que no tiene suciedad, burbujas, o cualquier otro defecto que pudiera alterar el rasgo biométrico.

  Para la cara, se deberá comprobar que la imagen contenga los puntos característicos de la cara (cejas, boca, ojos, nariz, etc.), que la imagen tenga buena calidad, sea nítida y tenga una iluminación adecuada.

- Si se quisiera realizar un estudio más profundo y preciso de la calidad de las muestras, existen algoritmos que facilitan esta tarea comparando la muestra real con la falsa realizando una serie de operaciones para determinar sus puntos característicos y posteriormente determinar cuánto de parecido es la muestra falsa a la muestra genuina.

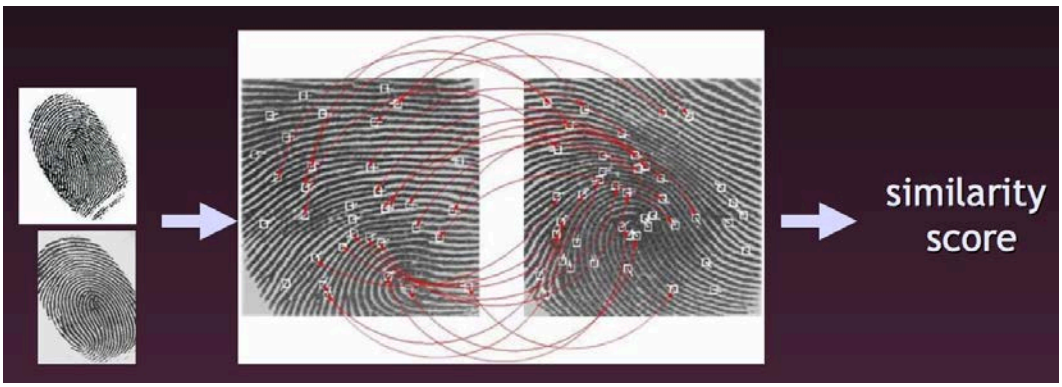


Figura 42. Comparación de muestra genuina y falsa [26]

En el caso de la huella existe el Nist fingerprint image quality (NFIQ) [26] que enfrentando la muestra biométrica genuina y la falsa devuelve un valor entre 1 y 5, correspondiente a la calidad de dicha muestra donde 5 sería el peor resultado y 1 el mejor.

Dichas valoraciones se basan en unos resultados de la FAR y la True Acceptance Rate (TAR) de la siguiente tabla:

Calidad	1- Excelente	2- Muy buena	3- Buena	2- Común	1- Mala
FAR	0,0037	0,0083	0,0131	0,0216	0,0477
TAR	0,997	0,994	0,993	0,9496	0,926

Tabla 11. Clasificación de la calidad de la huella basado en FAR y TAR [26]

Para que la calidad no sea un parámetro negativo en la muestra y su TAR sea de al menos un 99% se considera que las muestras como mínimo deben tener una NFIQ de nivel 3. De esta forma se aumenta el éxito del ataque enormemente mientras que con calidades peores (NIFQ 4 o 5) quedará en función de la FAR (Figura 43) el que su TAR sea alta o no.

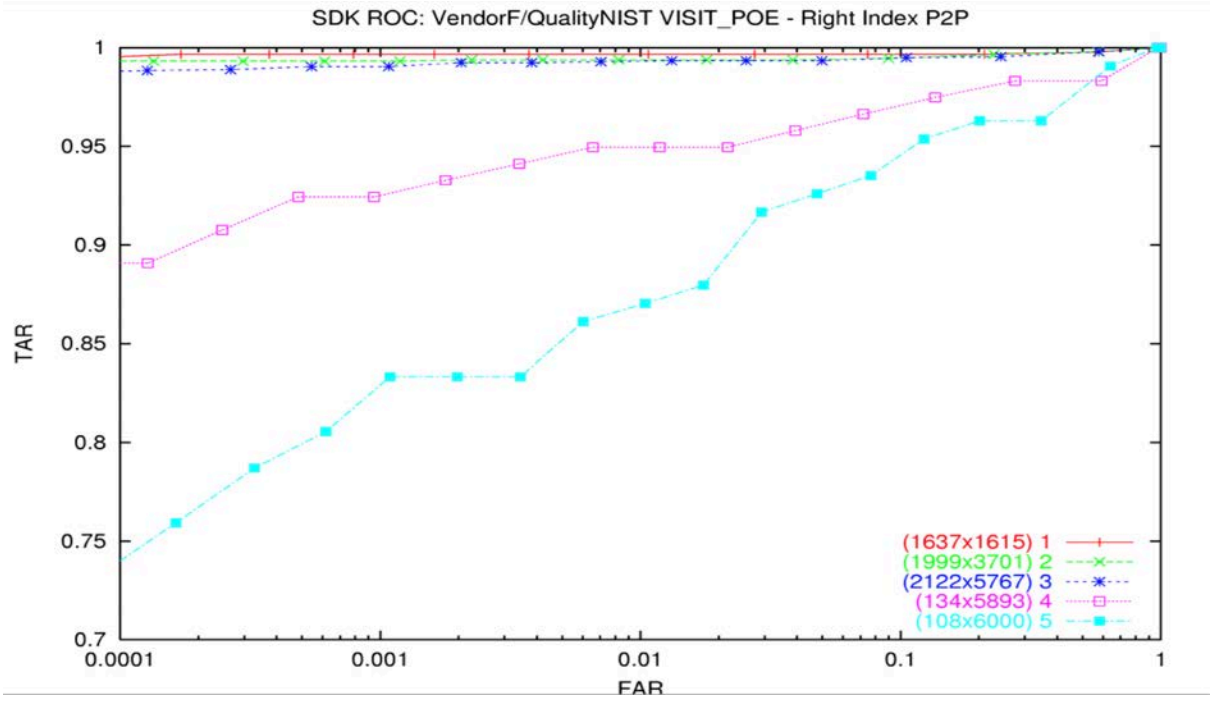


Figura 43. TAR frente a FAR para diferentes calidades de la huella [26]

- En el caso del reconocimiento facial existen otro algoritmos para garantizar la calidad como los basados en el estándar ANSI/NIST-ITL 1-2011 [27] que comprueban al igual que en huella, ciertos puntos geométricos característicos de la cara para establecer una de calidad relación entre la muestra genuina y la falsa. De nuevo, se debe garantizar la mayor calidad posible de la muestra.

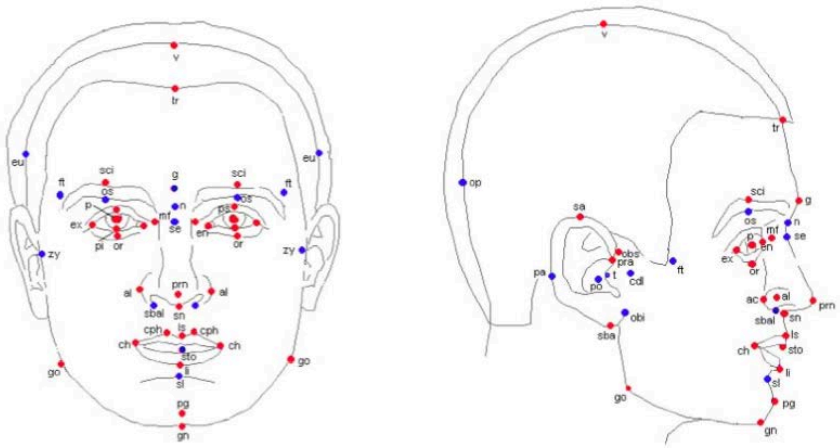


Figura 44. Puntos característicos de la cara [27]

- 3º Fase: Comprobar si el sistema detecta la muestra introducida

  - Se debe comprobar si el sistema detecta la muestra como el rasgo biométrico que debería ser. Es decir, en el caso que se está analizando que la huella falsa se reconozca como una huella en el sensor y que la imagen de la cara se reconozca como una cara en la cámara.

    Para obtener unos resultados significativos se ha decidido que por cada muestra deben realizarse 5 intentos. De esta forma se comprueba el Failure to detect (FTD), una tasa que devuelve el porcentaje de fallo del sistema al no reconocimiento de una muestra biométrica.

    Para realizar los intentos se deben probar diferentes combinaciones de posicionamiento. En el caso de la huella, rotarla, trasladarla y cambiar la presión. Para la cara, acercar o alejar la imagen o rotarla.

- 4º Fase: Comprobar si el sistema es capaz de capturar la muestra introducida

  - Se debe comprobar si el sistema es capaz de capturar la muestra introducida, no sólo de detectarla. Es decir, que la huella y la cara sean capturadas para un posterior procesamiento digital.

    Se ha decidido de nuevo que deben realizarse 5 intentos por cada muestra. De esta forma se comprueba el Failure to Capture (FTC), que devuelve el porcentaje de fallo del sistema a la no captura de una muestra biométrica.

Como se hizo en la anterior fase, si hay alguna posición en especial que aumente el éxito de detección de una muestra, es recomendable usar la misma posición para capturar.

- 5º Fase: Comprobar que realiza el procesamiento digital de la imagen y la comparación con la BBDD

  - Es el último paso de la fase de pruebas y directamente va asociada a la captura de la muestra, puesto que si es capaz de capturarla, es capaz de procesarla digitalmente. Realmente esta fase no está sujeta al evaluador, pero en teoría si la muestra tiene la calidad apropiada y no existe fallo al detectar ni al capturar, el ataque debería vulnerar el sistema. Los modos de procesamiento digital incluyen su comparación 1-1 en modo verificación y modo identificación 1-N.

Como se dijo anteriormente, se ha determinado que el éxito del ataque desde un punto de vista biométrico, tanto para el modo identificación como verificación, debe cumplir que el ataque vulnere el sistema al menos el 50% de los intentos. De esta forma se asegura que el suceso más probable es el de vulnerar el sistema.

Desde el punto de vista de la seguridad con que el ataque vulnere en alguna ocasión el sistema se considerará que es vulnerable. Es una valoración menos precisa puesto que lo que importa es si el sistema es vulnerable o no, no el porcentaje de veces que va a ocurrir como en el caso del punto de vista biométrico.

A continuación se realizan unas pruebas para ejemplificar esta metodología de evaluación de la seguridad.

4.4.1.1 Pruebas de reconocimiento facial

Puesto que no se disponía del sistema ABC real, las pruebas y los ataques correspondientes se ejecutaron en los sistemas disponibles en los laboratorios.

El sistema real tiene una cámara Logitech QuickCam Sphere AF y la cámara con la que se realizaron las pruebas era la Logitech Quickcam Fusion que cumple con los requisitos mínimos para el óptimo funcionamiento de los algoritmos faciales (resolución máxima de 1280x720 pixeles frente a 640x480 pixeles de resolución mínima, 24 bits true color frente a escala de grises 8 bits mínima y una captura de imágenes de hasta 20 FPS frente a 10 FPS mínimos).

En cuanto al algoritmo de reconocimiento facial, el sistema real usa VeriLook de Neurotechnology y las pruebas se realizaron con la versión gratuita de demostración del VeriLook 5.4. Pese a ser una versión gratuita cumple con los requisitos mínimos para garantizar resultados significativos (funciona en modo verificación o identificación, FAR= 0,01%, gestiona la calidad de las muestras obtenidas y tiene tolerancia a la traslación y rotación).

Dentro del propio VeriLook se usarán diferentes opciones de reconocimiento para determinar el rango en el cual el ataque propuesto tendría éxito y en cual no.

A continuación comienzan las pruebas en base a las fases anteriormente descritas:

- 1º Fase: Obtener las muestras biométricas falsas

Anteriormente se expuso que en el caso del sistema ABC español, puesto que abarca todos los sexos y todas las edades se necesitarán 12 mujeres y 12 varones, lo que corresponde a 2 mujeres y 2 varones de cada rango de edad.

Debido a la falta de medios y puesto que esto es un ejemplo de cómo se debe evaluar, sólo se harán las pruebas con 2 personas, un hombre y una mujer. Por cada uno de ellos, se tomarán 3 muestras de la cara realizando una fotografía.

Figura 45. Fotografía de la cara

- 2ºFase: Comprobar la calidad de las muestras falsas obtenidas

Para comprobar la calidad de las fotografías (ver figura 45) se debe asegurar que la imagen contiene toda la superficie de la cara, que tenga una expresión neutra, que la imagen sea de buena calidad, sea nítida y tenga una iluminación adecuada.

- 3º Fase: Comprobar si el sistema detecta la muestra introducida

Poniendo la cámara web enfrente de la fotografía, detecta perfectamente la cara en todas y cada una de las ocasiones que se prueba. Por lo tanto tiene un FTD = 0%. Esto es una buena señal puesto que significa que la calidad de la muestra biométrica falsa es buena y por eso lo reconoce como una cara.

Por otro lado, para probar unas condiciones más reales al sistema, se va a realizar un intento de verificación facial mediante video. En este caso, en vez de usar una fotografía para identificarse en el sistema, se usará un video. Donde se nuevo el FTD = 0%.

En las figuras 46 y 47 se puede observar el entorno de pruebas y la identificación de la imagen en el programa VeriLook.

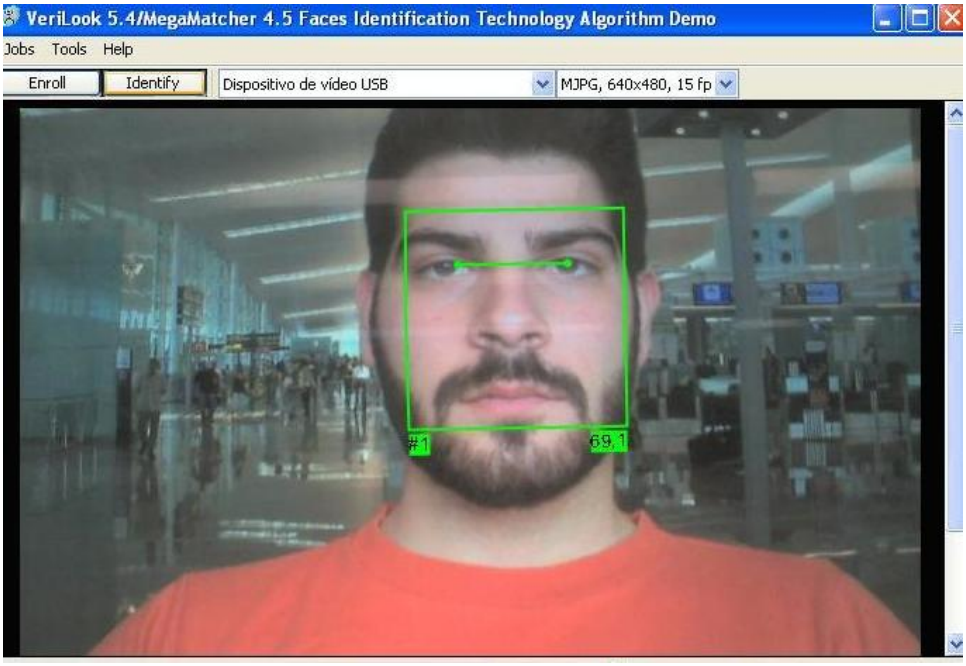


Figura 46. Reconocimiento de la muestra biométrica falsa (Foto)

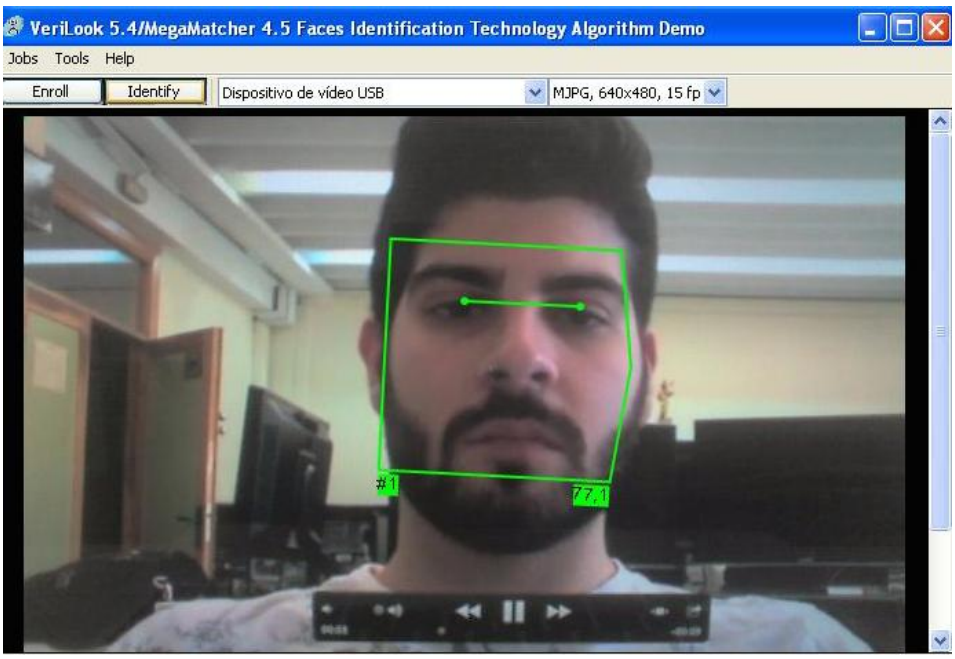


Figura 47.Reconocimiento de la muestra biométrica falsa (Video)

- 4º Fase: Comprobar si el sistema es capaz de capturar la muestra introducida

Aquí es cuando llega el primer problema. Puesto que el algoritmo es capaz de detectar si es una fotografía o no, no es capaz de reconocer al usuario por una sola fotografía ya que para la identificación utiliza un mínimo de 10 fotografías adquiridas mediante video para comparar con la BBDD. El FTC = 100% y por lo tanto, el sistema no es capaz de identificar al usuario. El ataque no vulnera el sistema con esta configuración.

Cambiando parámetros de la configuración del algoritmo se modifica para que la obtención de la muestra biométrica para la comparación con la BBDD, se realice con la obtención de una sola fotografía y no con 10 como ocurría antes. En ese caso, el sistema captura y acepta la muestra biométrica falsa. El FTC = 0%.

Por otro lado, para probar unas condiciones más reales al sistema se va a realizar un intento de verificación facial mediante video. En este caso, en vez de usar una fotografía para identificarse en el sistema, se usará un video. El sistema fallaba habitualmente a la hora de capturar la imagen, dando como resultado un FTC=80% después de la realización de todos los intentos con todas las muestras.

- 5º Fase: Comprobar que realiza el procesamiento digital de la imagen y la comparación con la BBDD

Como se dijo anteriormente, este proceso realmente no depende del evaluador y está íntimamente ligado con la fase de captura de la imagen, pues automáticamente después de capturar la imagen, la procesa para compararla con la BBDD.

En el caso del experimento con la fotografía resultó tener un FTP=0% después de realizar todas las pruebas. El sistema una vez compara al usuario con la BBDD devuelve un número entre 0 y 255 correspondiente a la similitud entre las muestras llamado Score. El Score medio fue de 94,8 (corresponde a una similitud del 37,25%), el Score máximo alcanzado de 116 (corresponde a una similitud del 45,49%) y el score mínimo de 83 (corresponde a una similitud del 31,76%).

Para el experimento con video, resultó no ser tan satisfactorio como el anterior. Después de realizar las pruebas se obtuvo un FTP=0% en las ocasiones que capturaba la muestra. El sistema una vez compara al usuario con la BBDD devuelve un número entre 0 y 255 (Score). El Score medio fue de 54 (corresponde a una similitud del 21,17%), el Score máximo alcanzado de 55 (corresponde a una similitud del 24,71%) y el score mínimo de 41 (corresponde a una similitud del 16,07%).

Para realizar una valoración de los resultados se necesita saber los umbrales de decisión para realizar la última operación lógica: Aceptar al usuario como genuino o rechazarlo como usuario impostor. Esto depende directamente del umbral seleccionado, en las pruebas se eligió 10 puesto que así se asegura la identificación y aceptación de la muestra pero no la vulneración del sistema.

Desde el punto de vista de la biometría, si el impostor es aceptado al menos un 50% de las veces como un usuario genuino el sistema es vulnerable mientras que para la seguridad, con que el impostor sea aceptado una vez, el sistema será vulnerable. Por lo tanto, el hecho de sea o no vulnerable está sujeto al umbral de decisión seleccionado en el sistema el cual será alto para aplicaciones de mayor seguridad y más bajo para aplicaciones comerciales.

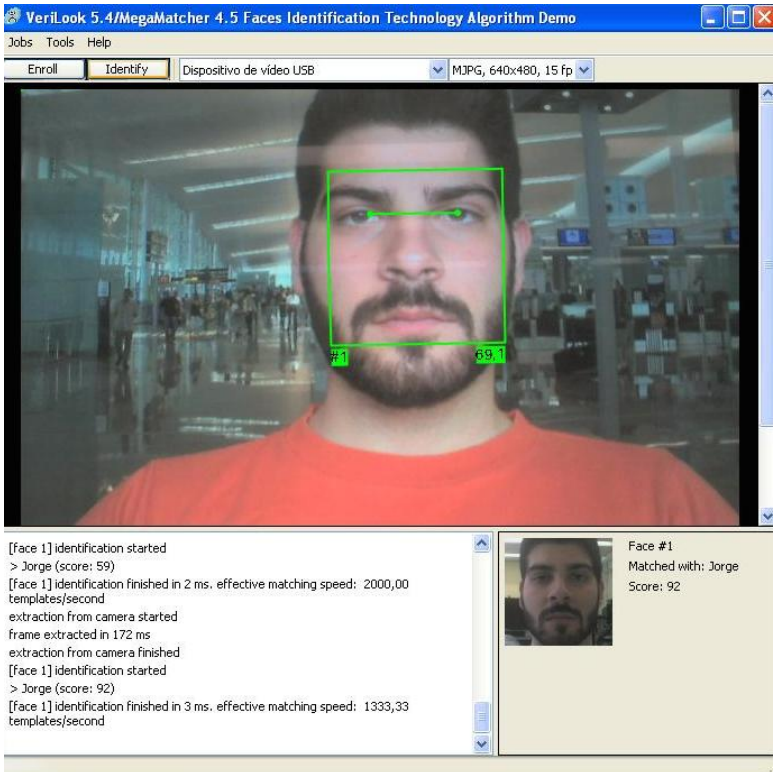


Figura 48. Identificación del usuario con foto

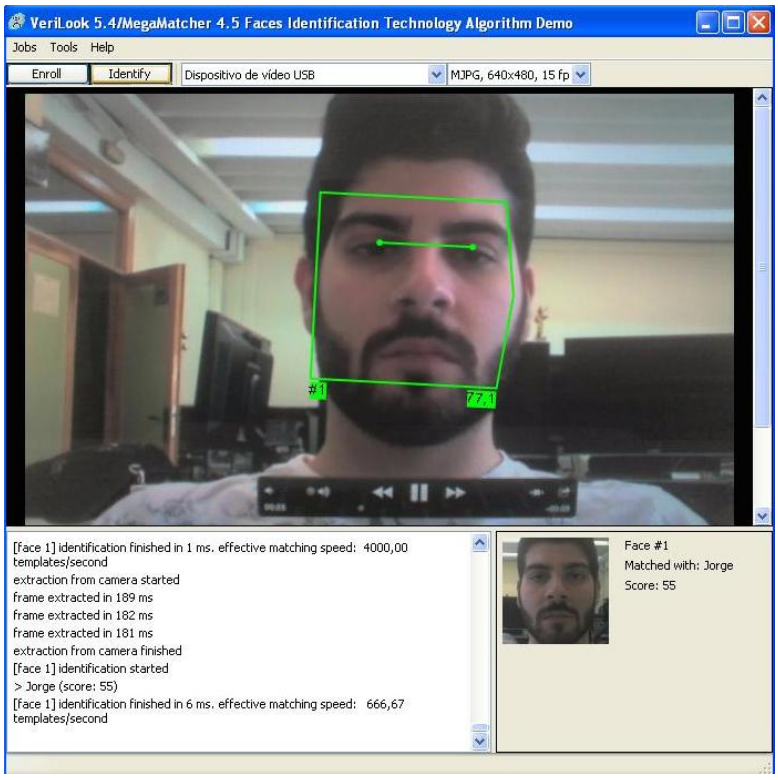


Figura 49. Identificación del usuario con video

4.4.1.2 Pruebas de reconocimiento dactilar

Puesto que no se disponía del sistema ABC real, las pruebas y los ataques correspondientes se ejecutaron en los sistemas disponibles en los laboratorios.

El sistema real tiene un sensor L SCAN 100 de Crossmatch y el sensor con el que se realizaron las pruebas era un Biometrika FX3000 que cumple con los requisitos mínimos para el óptimo funcionamiento de los algoritmos de reconocimiento dactilar (500 ppi, sensor óptico reflexivo, rango de funcionamiento con humedad 10-90% y temperatura 0-40ºC y resolución imagen de 600x600 pixeles).

En cuanto al algoritmo de reconocimiento dactilar, el sistema real usa VeriFinger de Neurotechnology y las pruebas se realizaron con la versión gratuita de Neurotechnology basado en VeriFinger. Pese a ser una versión de demostración cumple con los requisitos mínimos para garantizar resultados significativos (funciona en modo verificación o identificación, FAR= 0,01%, gestiona la calidad de las muestras obtenidas y tiene tolerancia a la traslación, rotación y deformación).

A continuación comienzan las pruebas en base a las fases anteriormente descritas:

- 1º Fase: Obtener las muestras biométricas falsas

Anteriormente se expuso que en el caso del sistema ABC español, puesto que abarca todos los sexos y todas las edades se necesitarán 12 mujeres y 12 varones, lo que corresponde a 2 mujeres y 2 varones de cada rango de edad.

Debido a la falta de medios y puesto que esto es un ejemplo de cómo se debe evaluar, sólo se harán las pruebas con 2 personas, un hombre y una mujer. Por cada uno de ellos, se tomarán 3 muestras de la huella por el método de Matsumoto.

Figura 50. Huella falsa por el método de Matsumoto

- 2ºFase: Comprobar la calidad de las muestras falsas obtenidas

El principal problema derivado del método de Matsumoto es la gelatina, puesto que tiende a formar burbujas lo que acaba produciendo una muestra biométrica de mala calidad. Para comprobar la calidad de las huellas se debe asegurar la nitidez de las líneas características (Delta y Core), que su textura sea la adecuada y que la muestra contenga la mayor superficie posible de la huella.

Se puede apreciar en la figura 51, la diferencia realizando una huella con y sin burbujas. Además la muestra con burbujas tiene una textura más dura lo que provocará consecuencias a la hora de capturar la huella. Más adelante se verá la calidad de la imagen en el sensor para cada caso y como su efectividad desciende tremendamente.

Figura 51. Muestras falsas de la huella

- 3º Fase: Comprobar si el sistema detecta la muestra introducida

En un caso normal, las muestras de mala calidad son descartadas para la realización de las pruebas, pero para ilustrar que la calidad de la muestra y la realización correcta de la copia de la huella es un factor determinante, también se incluirán las huellas de mala calidad en las pruebas.

Poniendo tanto las muestras de buena o mala calidad en el sensor, detecta perfectamente todas y cada una de las muestras en las ocasiones en las que se prueba. Por lo tanto, tiene un FTD = 0%. Esto es una buena señal puesto que significa que al menos se detecta la muestra biométrica falsa como lo que debería ser, una huella.

- 4º Fase: Comprobar si el sistema es capaz de capturar la muestra introducida

En el caso de las muestras de buena calidad, el sensor captura perfectamente en todas y cada una de las ocasiones en las que se prueba. La imagen capturada es relativamente nítida (ver figura 52). Tras las pruebas, tiene un FTC = 0%. Esto es una buena señal puesto que significa que captura una muestra falsa que tiene una gran calidad y por lo tanto se prevé un éxito en el reconocimiento con la muestra genuina.

Por otro lado, probando las muestras de mala calidad, se obtiene un FTC = 27%. Además como se puede observar en la figura 52, las burbujas aparecen en la imagen capturada creando poca uniformidad en las líneas características. El hecho de que también su textura no sea la adecuada, sino más dura, implica que hay que aplicar mayor presión para que el sensor capture toda la superficie y como resultado, que la imagen se oscurezca y sus líneas no queden bien definidas.

Figura 52. Calidad de las muestras capturadas : a) genuina, b) Falsa buena, c) Falsa mala

- 5º Fase: Comprobar que realiza el procesamiento digital de la imagen y la comparación con la BBDD

Como se dijo anteriormente, este proceso realmente no depende del evaluador y está íntimamente ligado con la fase de captura de la imagen pues automáticamente después de capturar la imagen, la procesa para compararla con la BBDD.

En el caso del experimento con la huella falsa de buena calidad resultó tener un FTP=0% después de realizar todas las pruebas. El sistema una vez compara al usuario con la BBDD devuelve un número entre 0 y 100 correspondiente a al porcentaje de similitud entre la muestra genuina y la falsa llamado Score. El Score medio fue de 63%, el Score máximo alcanzado de 79% y el score mínimo de 49%.

Para el experimento con la huella falsa de mala calidad, resultó no ser tan satisfactorio como el anterior. Después de realizar todas las pruebas e intentos obtuvo un FTP=0% en las ocasiones que capturaba la muestra. El Score medio fue de 13%, el Score máximo alcanzado de 17% y el score mínimo de 5%.

Figura 53. Prueba en el sensor de huella

Para realizar una valoración de los resultados obtenidos se necesita saber el umbral de calidad seleccionado para aceptar al usuario como genuino o rechazar como usuario impostor. En las pruebas se eligió 10 puesto que así se asegurará la identificación y aceptación de la muestra pero no vulneración del sistema.

Como se dijo anteriormente, desde el punto de vista de la biometría si el impostor es aceptado al menos un 50% de las veces como un usuario genuino el sistema es vulnerable mientras que para la seguridad, con que el impostor sea aceptado una vez, el sistema será vulnerable. Por lo tanto, el hecho de sea o no vulnerable está sujeto al umbral de score seleccionado en el sistema el cual será alto para aplicaciones de mayor seguridad y más bajo para aplicaciones comerciales.

Para el siguiente apartado, se va a suponer que el umbral de score seleccionado tanto para huella como para cara, es lo suficientemente bajo como para que en ambos casos (huella y cara) el sistema haya sido vulnerado al menos una vez. Por lo tanto, desde el punto de vista de la seguridad el sistema es vulnerable.

Gracias a dichas suposiciones se puede calcular la resistencia del TOE.

4.4.2 Cálculo de resistencia del TOE

Para determinar la resistencia del TOE a potenciales vulnerabilidades o ataques, se deberán usar aquellos ataques que hayan vulnerado el sistema satisfactoriamente. En el caso que se ha analizado, el ataque tenía un potencial total era Intermedio (ver Tabla 12) y ha vulnerado el sistema.

Valor	Potencial de ataque necesario para explotar el sistema:	Resistencia del TOE a ataques con potencial de nivel:	Seguridad frente a potenciales de nivel:	Fallo frente a potenciales de nivel:
0-9	Básico	Ninguno	-	AVA_AVAN.1 AVA_AVAN.2 AVA_AVAN.3 AVA_AVAN.4 AVA_AVAN.5
10-13	Intermedio	Básico	AVA_AVAN.1 AVA_AVAN.2	AVA_AVAN.3 AVA_AVAN.4 AVA_AVAN.5
14-19	Moderado	Intermedio	AVA_AVAN.1 AVA_AVAN.2 AVA_AVAN.3	AVA_AVAN.4 AVA_AVAN.5
20-24	Avanzado	Moderado	AVA_AVAN.1 AVA_AVAN.2 AVA_AVAN.3 AVA_AVAN.4	AVA_AVAN.5
25 o más	Profesional	Avanzado	AVA_AVAN.1 AVA_AVAN.2 AVA_AVAN.3 AVA_AVAN.4 AVA_AVAN.5	-

Tabla 12. Resistencia del TOE a los diferentes potenciales de ataque [9]

Aplicando la Tabla 12, se concluye que la resistencia del TOE es Básica. Esto quiere decir, que tendrá resistencia a ataques con potencial total Básico (AVA_AVAN.1 y AVA_AVAN.2) y que será vulnerable por ataques con potencial total Intermedio (AVA_AVAN.3), Moderado (AVA_AVAN.4), Avanzado (AVA_VAN.5) y Profesional (más que AVA_AVAN.5).

En este sentido no se concluye ni mucho menos que el sistema ABC tenga esta resistencia, sino que el sistema que se ha probado en el laboratorio tiene esa resistencia básica. Suponiendo además, un umbral de score que permita aceptar al usuario impostor como genuino ya que si dicho umbral fuera muy alto (lo normal en aplicaciones de alta seguridad) no se habría vulnerado el sistema y por lo tanto, tendría una resistencia más alta.

Aquí concluye la tercera y última fase de la evaluación de la seguridad de un sistema ABC.

4.5 Informe de seguridad

El estudio de la seguridad del sistema biométrico se da por finalizado porque se sabe cuál es el nivel de seguridad del sistema bajo evaluación y que tipo de ataques son propensos a vulnerarlo. Adicionalmente se incluye un informe final donde como evaluadores se dé una opinión de la seguridad del sistema y donde se propongan mejoras para incrementar su seguridad.

En primer lugar, una vez se han realizado las tres fases de la evaluación de la seguridad (1º Fase: Identificación de posibles vulnerabilidades, 2º Fase: Búsqueda y definición de ataques y 3º Fase: Penetración o pruebas) se podrá concluir cual es la resistencia del TOE. Puesto que las pruebas no se han realizado en el sistema ABC real no será una conclusión exacta de la seguridad de dichos sistemas, sino más bien del sistema del laboratorio que se ha utilizado suponiendo ciertas hipótesis.

Se ha concluido que la resistencia del TOE es Básica. Esto quiere decir, que tendrá resistencia a ataques con potencial total Básico (AVA_AVAN.1 y AVA_AVAN.2) y que será vulnerable a ataques con potencial total Intermedio (AVA_AVAN.3), Moderado (AVA_AVAN.4), Avanzado (AVA_VAN.5) y Profesional (más que AVA_AVAN.5). Pero en este sentido no se concluye ni mucho menos que el sistema ABC tenga esta resistencia. Además en el entorno de trabajo no se han tenido en cuenta estos factores:

- No se ha realizado verificación documental tanto óptica, para comprobar la autenticidad del documento, como lógica, para enfrentar la documentación con las bases de datos del CNP.
- El reconocimiento dactilar no se ha realizado con el mismo sensor, ni verificación MoC y no se ha usado el algoritmo VeriFinger.
- El reconocimiento facial no se ha realizado con la misma cámara, ni a la misma velocidad de captura de imágenes y no se ha usado el algoritmo VeriLook.
- Los umbrales de decisión seleccionados tanto para el reconocimiento facial y dactilar han sido muy bajos para realizar las pruebas. Sin embargo, en el sistema real, puesto que es una aplicación de alta seguridad, el umbral de decisión para aceptar a un usuario será mucho más exigente.
- No se han realizado los reconocimientos de forma secuencial de forma que los ataques tienen que vulnerar el sistema en la misma ocasión para tener éxito.
- Las pruebas se han realizado sin supervisión, mientras que en el sistema ABC habría vigilancia de agentes del CNP.

Teniendo en cuenta esas consideraciones, el ataque de reconocimiento facial no habría funcionado y por lo tanto, el sistema ABC tendría como mínimo una resistencia Intermedia y como máximo una resistencia Avanzada. Habría que seguir realizando ataques en condiciones más reales para seguir acotando la resistencia del sistema ABC español. Pero como se ha dicho anteriormente, por un lado, no se tienen los medios para realizar esos ataques y por otro lado, este TFG es una guía para la evaluación de la seguridad no una guía de cómo vulnerar un sistema ABC.

Una vez se acota la resistencia del sistema, se demuestra que existen ataques que pueden vulnerar el sistema y entonces existen dos opciones, incrementar o no la seguridad. Es posible que desde un punto de vista económico sea más rentable que sea vulnerable puesto que las pérdidas por un posible ataque son menores que la inversión para actualizar el sistema frente a la amenaza o que desde el punto de vista de un atacante, la inversión de realizar todo este estudio y ejecución es más alta al beneficio que va a conseguir vulnerando el sistema.

Como evaluador, se debe informar al propietario de los sistemas las posibles puntos débiles (objeto de vulnerabilidades) y también los puntos fuertes del sistema (no objeto de vulnerabilidades). En el caso de los sistemas ABC españoles:

- **Puntos fuertes**

  - La verificación documental: La única forma de vulnerar dicha verificación es o consiguiendo el documento original de la persona que se quiere suplantar (teniendo entonces que realizar copias falsas de los rasgos biométricos) o bien, un documento original realizado fraudulentamente con los datos de otra persona pero las muestras biométricas del falsificador almacenadas.

  - Alta protección para los ataques indirectos (ciber ataques): En primer lugar porque la verificación se realiza MoC, lo que elimina intermediarios en la comparación de las muestras biométricas y por ello la imposibilidad de intervenir en el proceso. Es posible que en el proceso de identificación con las BBDD del CNP se pudiera intervenir, pero pese a la poca información del tema debido a su naturaleza, se supone que debe haber buenos sistemas de seguridad frente a este tipo de ataques.

- **Puntos débiles**

  - Reconocimiento facial: En general, el reconocimiento facial no tiene tanta precisión y bajas tasas de error como otro tipo de reconocimientos biométricos pese a su intenso uso y su alta aceptación social. Si que se descartan los ataques con fotografías o videos pues el algoritmo es capaz de detectarlo, el sistema puede ser objeto de ataques con máscaras.

  - Reconocimiento dactilar: En general, el reconocimiento dactilar es muy discriminatorio y tiene bajas tasas de error comparado con otros sistemas biométricos. Los ataques que pueden vulnerar este sistema son los que introducen huellas falsas de buena calidad en el sensor (método de Matsumoto).

Por lo tanto, los dos posibles objetivos de ataques que pueden ser mejorados para incrementar la seguridad del sistema ABC y disminuir las potenciales vulnerabilidades, son el reconocimiento dactilar y el facial. Teniendo en cuenta el tipo de ataques que son más propensos a vulnerar el sistema (máscaras y huellas falsas realizadas con diversos materiales) se van a proponer mejoras para detectar precisamente ese tipo de ataques.

- **Posibles mejoras de reconocimiento facial**

  - Ampliar las imágenes de reclutamiento: Como se observó en el apartado 4.2.2.4 en el algoritmo VeriLook (ver figura 25, 26 y 27) la diferencia en los resultados cuando se compara con una sola imagen a comparar con cuatro imágenes, produce unos resultados significativamente mejores. Una solución sería un reclutamiento que se realice con cuatro fotografías y no sólo una. De esta forma se podrá incrementar el umbral del score para que el reconocimiento facial sea más preciso y exigente.

    La parte positiva de la mejora es que sólo es necesario ampliar el almacenamiento de las bases de datos a cuatro veces su capacidad lo que no supone un gran coste económico. Pero en cambio, tener una BBDD más grande también implica un mayor tiempo de procesamiento y de paso por la frontera, contradiciendo el objetivo de los sistemas ABC que es reducir las colas y tiempos de espera de los sistemas manuales.

  - Reconocimiento 3D: Como se comentó en el apartado 4.2.2.3 existen técnicas de reconocimiento basado en 3D para captar información sobre la forma de la cara. Posteriormente de identifican los rasgos característicos de la cara (la barbilla, el contorno de los ojos, la nariz o los pómulos, etc.), así como información espacial, la textura y la profundidad. Una de las ventajas del reconocimiento facial en 3D es que no les afectan los cambios de iluminación, como pasa en el caso de otras técnicas. Además, otro punto a favor es que pueden reconocer una cara en diferentes ángulos, incluso de perfil. Lo que garantizaría prácticamente al 100% la imposibilidad de generar una cara de forma tridimensional falsa.

    La viabilidad técnica no es del todo positiva ya que esta precisión del sistema conlleva que los sensores deben de estar muy bien calibrados y sincronizados constantemente para adquirir una imagen correctamente además de necesitar una alta velocidad de procesamiento. El desembolso inicial y el coste de mantenimiento son altos.

  - Cámara infrarroja: Incorporar una cámara infrarroja adicional para medir temperatura, porque la cara debido en parte al riego sanguíneo, tiene zonas más calientes que otras mientras que en las máscaras al no tener sangre, la superficie tiene una temperatura homogénea cercana a la temperatura ambiente y no a la corporal. Es una solución eficaz y barata.

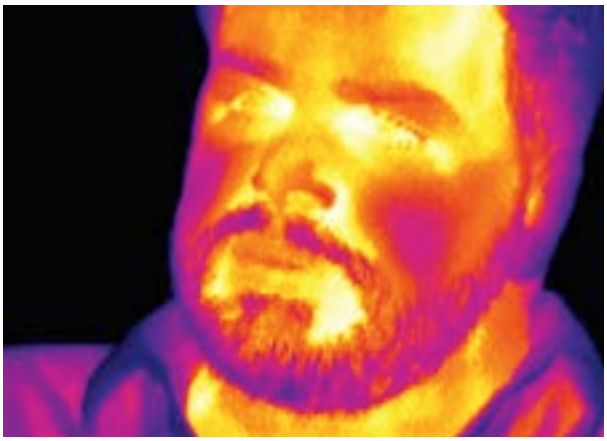


Figura 54. Imagen de temperatura de la cara

- **Posible mejora de reconocimiento dactilar**

  - Sensor óptico transmisivo: En un sensor de huella dactilar transmisivo, la humedad no produce ninguna dificultad. Ve a través de la superficie de la piel sobre una superficie más profunda y produce una imagen multiespectral. El uso de diferentes longitudes de onda para generar imágenes proporciona información de diferentes estructuras subcutáneas, indicación de que el objeto en cuestión es un dedo genuino. Sólo unos dedos artificiales muy precisos podrían vulnerar este tipo de sensor, evitando así la mayoría de ataques que implican huellas artificiales como el método de Matsumoto.

    Su viabilidad técnica es positiva ya que tan sólo sería cambiar un tipo de sensor por otro y además el desembolso sería relativamente bajo.

A modo de conclusión del informe de seguridad, ya se ha acotado la resistencia o seguridad del sistema. Se han remarcado cuáles son sus puntos débiles, posibles objetivos de ataques y por lo tanto, de ser vulnerables. Se han planteado las posibles soluciones para mejorar la seguridad donde existe mayor probabilidad de ataques exitosos.

El trabajo del evaluador ha terminado. A partir de este informe, será decisión del propietario del sistema incrementar o no la seguridad con las medidas propuestas u otras.

5 Conclusiones y líneas futuras

En este último capítulo se hará una conclusión sobre el trabajo realizado, qué problemas se han encontrado en el camino y cómo finalmente se han resuelto. Además se determinarán las futuras líneas de investigación en torno a la metodología de evaluación de la seguridad tanto en sistemas biométricos como en sistemas ABC.

5.1 Conclusiones

La fiabilidad y seguridad en los métodos de identificación de personas se han convertido en una necesidad clave en la sociedad interconectada en la que se vive. Frente a esta necesidad, los sistemas automáticos de reconocimiento biométrico han venido sustituyendo, cada vez más rápido desde las últimas décadas, a los sistemas de identificación tradicionales (basados en tarjetas de identificación o claves). El uso de rasgos biométricos altamente discriminantes (huella, cara e iris) se han impuesto en los sistemas multi biométricos para aplicaciones de alta seguridad, como los sistemas automáticos de control de fronteras. Pese a su tremendo auge, la evaluación de rendimiento y/o seguridad no es una práctica muy común debido a su complejidad.

En este proyecto se ha realizado el diseño, por un lado, de una metodología para la evaluación completa de la seguridad de un sistema biométrico y por otro lado, la validación e implementación de esta metodología aplicada a los sistemas ABC y el control de fronteras. Esto último, proporciona una solución más tangible para la evaluación de la seguridad ya que, la metodología en general, puede resultar abstracta y compleja.

Los principales problemas que han surgido durante el desarrollo del trabajo, sobre todo han estado referidos a las partes del proyecto de las que no se tenía una base en la que apoyarse. Puesto que la metodología de evaluación del rendimiento o seguridad no es un tema muy tratado o común y en ocasiones abstracto y complejo, la búsqueda de información y documentación fue intensa y difícil. Sin embargo, el descubrimiento de Common Criteria supuso un punto de inflexión en el TFG pues asentó una base sólida para el desarrollo de la metodología.

Debido a la importancia de la evaluación de sistemas biométricos y más para aplicaciones como el control de fronteras, se espera que sea el apoyo necesario para los presentes y futuros evaluadores que quieran hacer un estudio riguroso de la seguridad de un sistema biométrico. Además, este trabajo puede utilizarse como ilustración de las carencias que tenía la biometría en torno a la seguridad, de forma que se supone un primer punto de partida para que los evaluadores puedan mejorar el proyecto y conseguir en un futuro próximo un estándar o guía mucho más detallada y completa.

Por último, y como conclusión personal, el alumno partía desde un desconocimiento absoluto del tema a tratar, y concluye el trabajo con los conocimientos y habilidades suficientes para poder seguir investigando en el terreno de las metodologías de evaluación, por lo que su consideración es que se han cumplido todos los objetivos, tanto técnico como personales, especificados al inicio del presente documento.

5.2 Líneas futuras de investigación

A partir del trabajo realizado en el ámbito de este proyecto, se abren nuevas líneas de investigación. Las más interesantes se detallan a continuación:

- Evaluar más modalidades de reconocimiento biométrico: No todos los sistemas ABC o sistemas multi biométricos contienen reconocimiento facial y dactilar, sino que existen otros muchos (iris, voz, geometría palmar, reconocimiento vascular, etc.). Una futura línea de investigación es analizar las vulnerabilidades de todos los tipos de reconocimiento biométrico, desarrollando ataques y definiendo un estándar para la evaluación de cualquier rasgo biométrico como modo de reconocimiento.

- Evaluar ataques indirectos: En este TFG no se han contemplado profundamente los ataques indirectos o ciber ataques. Una futura línea de investigación es el análisis de las vulnerabilidades de los sistemas informáticos tanto de los sistemas biométricos como de los sistemas ABC.

- Pruebas con diferentes condiciones ambientales: Debido a que los sistemas ABC suelen tener unas condiciones estables estándar no se han tenido demasiado en cuenta diferentes factores ambientales que podrían alterar el funcionamiento de los sistemas. Una futura línea de investigación es analizar diferentes modalidades de reconocimiento biométrico frente a altas/bajas temperaturas, a vibraciones o a diferentes presiones atmosféricas.

- Verificación documental: Una futura línea de investigación puede centrarse en evaluar ataques, la falsificación de documentos (DNI e o Pasaporte electrónico) y la búsqueda de contramedidas para evitar la aceptación de documentos falsos.

- Complementar la metodología: Con todas las anteriores líneas de investigación, realizar una evaluación complementada con todas las modalidades de reconocimiento biométrico, con ataques indirectos, con pruebas de los sistemas reales en diferentes condiciones ambientales y con ataques y vulnerabilidades de la verificación documental.

Bibliografía

[1] International Organization for Standarization, ISO/IEC 19795 – 1: 2006, *Information Technology – Biometric performance testing and reporting – Part 1: Principles and frameworkd*, 2006.

[2] Common Criteria Biometric Evaluation Methodology Working Group, *Biometric Evaluation Methodology Supplement (BEM*), 2002.

[3] International Organization for Standarization, ISO/IEC 19792 – *Information Technology – Security techniques – Security Evaluation of biometrics*, 2009.

[4] Biometric Institute, *Biometric Vulnerability: A Principled Assessment Methodology*, Biometric Institute Ltd., 2008.

[5] Common Criteria, *Common Methodology for Information Technology Security Evaluation*, Version 3.1, Revision 4, 2012.

[6] *Trusted Biometrics under Spoofing Attacks (TABULA RASA)*, http://www.tabularasa-euproject.org, 2007-2013.

[7] Anil K. Jain, Arun Ross, and Salil Prabhakar. *An introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology*., 14(1), 2004.

[8] S. Nanavati, M. Thieme, and R. Nanavati. *Biometrics: Identity, verification in networked world*. Wiley, 2002.

[9] Common Criteria, *Characterizing Attacks to Fingerprint Verification Mechanisms*, Version 3.0, 2011.

[10] Wikipedia la enciclopedia libre. *Curva ROC*. http://es.wikipedia.org/wiki/Curva_ROC , Consultado: “12 de mayo de 2014”.

[11] Wikipedia la enciclopedia libre. *Ataque Hill-Climbing*. http://en.wikipedia.org/wiki/Hill_climbing Consultado: “12 de mayo de 2014”.

[12] European Agency for the Managment of Operational Cooperation at the external Borders of the member States of the European Union, *Best practice Operational Guidelines for Automated Border Control (ABC) Systems*, Version 2.0, 2012.

[13] Ministerio del interior (Secretaría de estado de seguridad), *Pliego de preinscripciones técnicas para la contratación de diseño y desarrollo de software para la adaptación de las actuales soluciones que componen la funcionalidad del sistema piloto de control automatizado de fronteras exteriores y su integración dentro de los sistemas de información del cuerpo nacional de policía*, 2011.

[14] Wikipedia, la enciclopedia libre. *Sensor de huella digital*. http://es.wikipedia.org/wiki/Sensor_de_huella_digital Consultado: "1 de Junio de 2014".

[15] Crossmatch, *Brochure L SCAN 100/100R*, Version 1,2006.

[16] Wikipedia, la enciclopedia libre. *Sistemas de reconocimiento facial.* http://es.wikipedia.org/wiki/Sistema_de_reconocimiento_facial Consultado: "1 de Junio de 2014".

[17] Logitech, *Brochure Logitech QuickCam Sphere AF*. http://www.logitech.com/es-es/support/quickcam-sphere-af Consultado: "1 de Junio de 2014".

[18] Neurotechnology, *Spanish Airports install multi-biometric security systems – Case Study*, 2010.

[19] Neurotechnology, *Verifinger SDK Brochure*. http://www.neurotechnology.com/verifinger.html Consultado: "3 de Junio de 2014".

[20] Neurotechnology, *VeriLook SDK Brochure.* http://www.neurotechnology.com/verilook.html Consultado: "4 de Junio de 2014".

[21] Ministerio del interior, Cuerpo Nacional de Policia, *DNI electrónico*. http://www.dnielectronico.es/Preguntas_Frecuentes/segur/# Consultado: "10 de Junio de 2014"

[22] Tsutomy Matsumoto, *Impact of Artificial "Gummy" Fingers on Fingerprint*, 2002.

[23] Shonagh Scott, *How To Cast The Face – Tutorial*. https://www.youtube.com/watch?v=TPPAg_GevaY Consultado: "10 de Junio de 2014".

[24] Stdot, *How to create a "gummy" fringerprint with PCBs*. http://www.stdot.com/pub/ffs/hack3.html Consultado: "10 de Mayo de 2014".

[25] ThatsMyFase, *Wearable Masks from a Photo*. http://www.thatsmyface.com/Custom-made-Wearable-Masks-From-a-Photo/View-all-products.html Consultado "10 de mayo de 2014".

[26] Elham Tabbasi Image Group - NIST, *NIST Fingerprint Image Quality and relation to PIV*, 2005.

[27] National Institute of Standards and Technology, *NIST fingerprint Testing and Standards*, 2013.

Anexo A: Planificación y Presupuesto

A continuación se va a llevar a cabo un desglose de las tareas que se han realizado a lo largo de este trabajo fin de grado, lo que facilitará posteriormente un cálculo aproximado sobre su coste.

A.1 Planificación

Debido a la complejidad de un trabajo de estas características se ha optado por dividirlo en distintas fases, las cuales se van a comentar a continuación:

Fase 1: Documentación inicial (65 horas)

I. Búsqueda y documentación sobre sistemas de reconocimiento biométrico, especialmente de los sistemas ABC (20 horas)

II. Búsqueda y documentación de metodologías de evaluación (15 horas)

III. Búsqueda y documentación sobre vulnerabilidades de los sistemas biométricos (15 horas)

IV. Búsqueda y documentación de ataques publicados (15 horas)

Fase 2: Desarrollo de la metodología de evaluación de la seguridad (100 horas)

I. Metodología de evaluación para sistemas biométricos (60 horas)

II. Metodología de evaluación para sistemas ABC (40 horas)

Fase 3: Pruebas de la metodología (70 horas)

I. Prueba de metodología en sistemas ABC españoles (40 horas)

II. Realización de pruebas de reconocimiento dactilar (15 horas)

III. Realización de pruebas de reconocimiento facial (15 horas)

Fase 4: Elaboración de la memoria (125 horas)

I. Redacción de la memoria (100 horas)

II. Corrección y maquetación (25 horas)

FASES	HORAS EMPLEADAS
Documentación inicial	65
Desarrollo de la metodología de evaluación de la seguridad	100
Pruebas de la metodología	70
Elaboración de la memoria	125
TOTAL	**360**

Tabla 13. Desglose de tareas

A.2 Presupuesto del Trabajo Fin de Grado

A.2.1 Costes materiales

Los materiales necesarios para la realización del TFG han sido en primer lugar un ordenador de altas prestaciones para el correcto funcionamiento de las labores de identificación y verificación en las pruebas, para la documentación y búsqueda de información y la redacción del proyecto. También se utilizó un sensor de huella dactilar Biometrika FX3000 para la realización de las pruebas de reconocimiento dactilar y una cámara web Logitech QuickCam Fusion para la realización de las pruebas de reconocimiento facial. Por último, también la compra de materiales utilizados en las pruebas (gelatina, agua, alginato dental y papel). Considerando un periodo de amortización de cada uno de los dispositivos de 3 años y teniendo en cuenta el tiempo del proyecto, los costes materiales quedan como se expone en la Tabla 14.

CONCEPTO	PRECIO (€)
Ordenador de altas prestaciones	200
Sensor Biometrika FX3000	36,67
Cámara web Logitech QuickCam Fusion	13.33
Material para pruebas	25
TOTAL	**275**

Tabla 14 – Costes Materiales

A.2.2 Costes de personal

Para la realización de este trabajo, ha sido necesaria la presencia de un jefe de proyecto y un ingeniero.

OCUPACIÓN	HORAS	PRECIO/HORA	IMPORTE (€)
Jefe de proyecto	35	50	1750
Ingeniero	360	30	10800
TOTAL	**395**		**12550**

Tabla 15 – Costes de Personal

A.2.3 Costes totales

Sumando los costes materiales más los costes de personal, añadiéndole costes indirectos, de un 20%, y el IVA, de un 21%, el proyecto tiene un coste total reflejado en la Tabla 16.

CONCEPTO	PRECIO (€)
Costes de materiales	275
Costes de personal	12550
Costes indirectos (20%)	2565
Subtotal	15390
IVA (21%)	3231.9
TOTAL	**18621.9**

Tabla 16 – Costes Totales

El coste total del proyecto es de DIECIOCHO MIL SEISCIENTOS VEINTIÚN EUROS CON NUEVE CÉNTIMOS.

Leganés, 20 de Junio del 2012

El ingeniero